E-Commerce and Internet Law: A Primer

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

The State Bar of California
2nd Annual Spring Meeting

April 27 & 28, 2001
La Jolla, CA

by Ian C. Ballon*
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

1001 Page Mill Road, Bldg. 2 Palo Alto, CA 94304-1006 Palo Alto Direct Dial: (650) 812-1389 (650) 213-0260	11355 West Olympic Boulevard Los Angeles, CA 90064-1614 Los Angeles Direct Dial: (310) 312-4326 (310) 312-4224 (310) 312-4224

June 2000

An earlier version of this paper was published by the American Bar Association in the book "The Performing Art of Advocacy: Creating A New Spirit" and presented at the 1995 ABA Annual Convention in Chicago, Illinois in conjunction with the program "Litigating in a Cyberspace World." The materials in this outline have been incorporated in the 3 volume legal treatise, "E-Commerce and Internet Law" by Ian C. Ballon, published by Glasser LegalWorks. For information on the book, contact Glasser LegalWorks at (800) 308-1700. The opinions expressed are solely those of the author.

OUTLINE

OUTLINE

A. Statutory Background

1. U.S. copyright law protects expression, but not underlying ideas
2. Copyright protection extends to:
    a. Original works of authorship
    b. Fixed in a tangible medium of expression
3. Copyright protection may be obtained for:
    a. Literary works
    b. Musical works, including any accompanying words
    c. Dramatic works, including any accompanying music
    d. Pantomimes and choreographic works
    e. Pictorial, graphic and sculptural works
    f. Motion pictures and other audiovisual works
    g. Sound recordings
    h. Architectural works
4. Copyright protection does *not* extend to any idea, procedure, process, system
5. Exclusive rights in copyrighted works
    a. to reproduce the copyrighted work in copies or phonorecords
    b. to prepare derivative works based upon the copyrighted work
    c. to distribute copies or phonorecords of the copyrighted work to the public
    d. to perform the copyrighted work publicly e. to display the copyrighted work publicly
    f. to perform the copyrighted work publicly by means of a digital audio transmission
6. Exception to a copyright owner's exclusive rights: archival or back-up copies of software and temporary copies created for maintenance or repair

B. Derivative Works and Multimedia Clearance

1. Definition
2. Multimedia works often are "derivative works"
3. Clearance
4. Digital technology challenges traditional copyright law

C. Software Infringement

1. What is protectable?
    a. Menu command hierarchies
    b. Icons
    c. Use of windows
    d. Use of menus
    e. Opening and closing of objects
    f. A computer animated key pad
    g. Constants
    h. Databases
    i. Input/output formulas
    j. Threshold values
2. Audiovisual works: screen displays and interfaces
    a. Screen displays may be protectable as audiovisual works.
    b. Interfaces protected as audiovisual works
3. What constitutes infringement?
    a. Elements
    b. Ownership
    c. Infringement by literal code copying
    d. Infringement by non-literal copying/"look and feel" infringement

e. Infringement based on exceeding the scope of a license/ "virtual identicality" required in some instances
f. Infringement through unauthorized importation
g. Infringement via the Internet

D. Liability Under the Computer Software Rental Amendments Act

1. The Computer Software Rental Amendments Act
2. *Central Point Software, Inc. v. Global Software & Accessories, Inc.*
   a. The first case decided under the Computer Software Rental Amendments Act
   b. Deferred billing
   c. Software upgrades
3. The opportunities for "sham" software transactions over the Internet

E. The Fair Use Defense

1. What constitutes fair use?
2. Reverse engineering of software
3. Parody
4. Taping television transmissions for future viewing
5. Photocopying articles for convenience
   a. 1994 opinion
   b. Amended opinion
   c. Law lags behind technology
   d. Implications online
6. The retransmission over the Internet of infringing material (the Church of Scientology cases)
   a. *Religious Technology Center v. F.A.C.T.Net, Inc.*
   b. Netcom litigation - the individually named defendant
   c. Netcom litigation - the internet access provider
   d. Lerma - initial orders
   e. Lerma - First Amendment arguments
   f. *Religious Technology Center v. Ward*
7. Web browsing
8. Shareware
9. Copying by visual search engines

F. The Third-Party Liability of Online Content and Access Providers

1. Direct Liability
   a. Strict liability
   b. Volitional conduct required
2. Culpable conduct required for contributory infringement
3. Vicarious liability
   a. NII White Paper
   b. Canadian position
   c. Further analysis
4. *Playboy Enterprises, Inc. v. Frena*
   a. Facts
   b. Holding
5. *Sega Enterprises Ltd. v. MAPHIA*
   a. Facts
   b. Holding
   c. Isolated acts of infringement
6. *Frank Music Corp. v. CompuServe Inc.*
   a. . Plaintiff's claims
   b. Settlement terms
7. *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*
   a. Procedural Background
   b. November 1995 opinion

c. Facts relevant to the motions
d. Erlich's transmissions held to create "copies" on Klemesrud's BBS and Netcom's computers
e. Netcom not liable for direct infringement
f. Netcom's potential liability for contributory infringement
g. Netcom not liable for vicarious infringement
h. Netcom's First Amendment argument
i. Netcom's fair use defense

8. Netcom Settlement
9. *Sega Enterprises Ltd. v. MAPHIA*
   a. Direct liability
   b. Contributory liability
10. *Sega Enterprises Ltd. v. Sabella*
11. *Playboy Enterprises, Inc. v. Webbworld, Inc.*
   a. Facts
   b. Initial ruling
   c. Trial decision - direct liability
   d. Trial decision - vicarious liability
   e. Vicarious of liability investors

G. Liability Limitations Under the Digital Millennium Copyright Act

1. Copyright Liability Limitations
2. Exemption from Liability (under any theory of law) for Removing or Disabling Access to Content
3. Threshold Requirements
4. Procedures for Notification and Counter Notification
5. Benefits for Service Providers
6. Benefits for Copyright Owners
7. More Information

H. Electronic Republication of Articles

1. *Tasini v. New York Times Co.*
2. Today it is common for publishing contracts to expressly define the parties' respective electronic publishing rights

I. Criminal Copyright Infringement

1. *United States v. LaMacchia*
   a. Facts
   b. Criminal copyright liability must be predicated on commercial exploitation
   c. The wire fraud statute was not applicable
   d. Civil liability
2. NET Act

III. TRADEMARK AND TRADE DRESS PROTECTION IN CYBERSPACE

A. Traditional Trademark Infringement on the Internet

1. Elements of an infringement claim
2. *Playboy Enterprises, Inc. v. Frena*
   a. Facts
   b. Trademark infringement - file descriptors
   c. Unfair competition
   d. Reverse "passing off
   e. Comparison to Ninth Circuit rule on reverse "passing off
3. *Sega Enterprises Ltd. v. MAPHIA*
   a. Facts
   b. Holding
   c. False designation of origin
4. *Sega Enterprises Ltd. v. Sabella*
   a. Facts

b. Trademark infringement
c. False designation of origin
d. State law claims

5. Contributory trademark infringement
   a. Contributory trademark infringement
   b. No liability for offering an Internet-related service.
   c. Actual knowledge

B. Dilution in Cyberspace

1. Elements of a claim
   a. Is a mark distinctive and famous?
   b. Split in the circuits
   c. Niche market fame
   d. Dilution defined
2. Defenses
3. Relief
4. Implications Online

C. Internet Domain Names

1. Lack of vigilance by trademark owners
   a. mcdonalds.com
   b. mci.com
   c. kaplan.com
2. Over-registration
3. Early litigation over rights in domain names
   a. *MTV Networks v. Curry*
   b. *Council of Better Business Bureaus, Inc. v. Sloo*
   c. *Fry's Electronics, Inc. v. Octave Systems, Inc.*
   d. *KnowledgeNet, Inc. v. Boone*
   e. *Wired v. Wire*
4. Trademarks as domain names
5. NSI's 1995 Domain Dispute Resolution Policy Statement
   a. Reservation of names
   b. Trademark infringement
   c. Indemnification
   d. Arbitration
   e. Results of the 1995 policy
   f. Fees
6. Litigation arising out of NSI's 1995 Domain Dispute Policy Statement
   a. *Roadrunner Computer Systems, Inc. v. Network Solutions, Inc.*
   b. *Clue.com.*
   c. *Giacalone v. Network Solutions, Inc.*
   d. *The Comp Examiner Agency, Inc. v. Juris, Inc.*
   e. *Avon Products v. Carnetta Wong Associates*
7. Domain names as trademarks
8. 1996 Domain Dispute Policy Statement.
   a. Hold procedures
   b. Definition of "registered"
   c. Interpleader-style action
   d. Court order binding
9. The 1998 Policy Statement
   a. Registration on the principal registry "or equivalent registry" required
   b. Litigation freezes the status quo ante
   c. Foreign lawsuits will stay NSI action
10. Domain name Dilution.
   a. Blurring

b. Tarnishment
c. No dilution will be found where a competing use does not diminish the value of a mark
11. Cybersquatting
a. *Panavision Int'l, L.P. v. Toeppen*
b. *Avery Dennison Corp. v. Sumpton*
12. Typographical errors
13. Use in commerce
14. What constitutes likelihood of confusion
a. Initial interest confusion
b. *Data Concepts, Inc. v. Digital Consulting, Inc.*
c. *Hasbro, Inc. v. Clue Computing, Inc.*
d. Case-sensitive domain names
15. Registrars' duties to trademark owners
16. In rem actions to recover domain names
a. *Umbro Int'l, Inc. v. 3263851 Canada, Inc.*
b. *Porsche Cars North America, Inc. v. Porsch.com*
c. *Dorer v. Arel*
17. ICANN Uniform Domain Name Dispute Resolution Policy

D. The Anticybersquatting Consumer Protection Act of 1999
1. Bad faith registration, trafficking or use of a domain name
a. Remedies
b. Statutory damages
2. *In Rem* Relief
a. Remedies limited
b. Extra-judicial relief/Registrar Liability
c. Constitutionality upheld
3. Protection for the names of individuals
a. Remedies
b. Prospective application
4. Liability limitations for domain name registrars and registries

E. Trademark Liability for Metatag Infringement
1. *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*
2. *Playboy Enterprises, Inc. v. Calvin Designer Label*
3. *Playboy Enterprises, Inc. v. Welles*

F. Key Words and Banner Advertisements

G. Trade Dress Protection for Screen Displays and Web Site Interfaces
1. Trade dress
2. Trade dress protection
3. Functionality
4. Timing may be critical
5. Case law
a. *Engineering Dynamics, Inc. v. Structural Software, Inc.*
b. *Computer Care v. Service System Enterprises, Inc.*
c. *Interactive Network, Inc. v. NTN Communications, Inc.*
d. *Brown Bag Software v. Symantec Corp.*
e. *Midway Manufacturing Co. v. Dirkschneider*
f. Recent decisions
6. The Internet's transformation of trade dress infringement claims

H. Fair Use (Including Consumer Criticism and First Amendment Issues)

IV. THE LAW OF CACHING, LINKING, FRAMING AND CONTENT AGGREGATION

A. Caching

B. Hypertext Links
1. Definition
2. Linking compared to caching
3. Lanham Act Liability

C. Framing
1. Definition

D. Copyright and Related Cases
1. *Shetland Times Ltd. v. Wills*
2. *Futuredontics, Inc. v. Applied Anagramics, Inc.*
3. *Bernstein v. J.C. Penney, Inc.*
4. *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*
5. *Ticketmaster Corp. v. Tickets.com Inc.*

E. Lanham Act and Related Cases
1. Deep Linking
   a. *Ticketmaster Corp. v. Microsoft Corp.*
   b. *Ticketmaster Corp. v. Tickets.com, Inc.*
2. Framing
   a. *The Washington Post Co. v. TotalNews, Inc.*
   b. *Hard Rock Café Int'l Inc. v. Morton*
3. *Playboy Enterprises, Inc. v. Universal Tel-A-Talk, Inc.*
4. *Bally Total Fitness Holding Corp. v. Faber*
5. *Archdiocese of St. Louis v. Internet Entertainment Group, Inc.*
6. *OBH, Inc. v. Spotlight Magazine, Inc.*
7. *Nissan Motor Co. v. Nissan Computer Corp.*

F. Technological Self-Help

G. The Digital Millennium Copyright Act.

H. Content Aggregation
1. *eBay, Inc. v. Bidder's Edge, Inc.*
2. FTC Investigation
3. *Storm Impact, Inc. v. Software of the Month Club*
4. Evaluating potential claims

I. Visual Search Engine Practices

V. MISAPPROPRIATION OF TRADE SECRETS IN CYBERSPACE

A. Definition
1. State law
2. What is a trade secret?
   a. Restatement of Torts
   b. California statutory definition.
3. Elements of a cause of action.
   a. General principles
   b. A California cause of action

B. Secrecy Required
1. Disclosure destroys the secret
2. Modern standard: reasonable protection
3. A company's failure to following its own procedures

C. Trade Secrets Posted over the Internet

1. *Religious Technologies Center v. Lerma*
2. *Religious Technology Center v. F.A.C.T.Net, Inc.*
3. *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*
4. *Ford Motor Co. v. Lane*

D. Trade Secrets Transmitted By Email

E. Commercially Marketed Software

F. The Inevitable Disclosure Doctrine

1. Legal Basis
2. State by State Review
3. *Doubleclick, Inc. v. Henderson*
4. Internet Applications of the Doctrine

VI. SOFTWARE PATENTS

A. Overview

B. What is Patentable?

C. Computer Software and Internet Business Models

D. Patent Protection Can Be Lost Through Premature Disclosure

E. Internet Patent Litigation

1. *Interactive Gift Express, Inc. v. CompuServe, Inc.*
2. . *E-data Corp. v. Micropatent Corp.*

VII. LICENSES AND ANTITRUST CONSTRAINTS

A. Software and Information

1. The First Sale Doctrine
2. Shrink wrap and click through licenses
    a. Consumer software licenses
    b. Unconscionability
    c. UCITA and the UETA
3. Infringement by exceeding the scope of a license
4. Breach of contract
5. Website Terms and Conditions

B. Music Available Over the Internet

1. In General
2. Webcasting
3. Downloadable Music/ MP3 Files
    a. Litigation
    b. SDMI
    c. DMCA anti-piracy provisions
4. Case Law
    a. *RealNetworks, Inc. v. Streambox, Inc.*
    b. *Universal City Studios, Inc. v. Reimerdes*
    c. *UMG Recordings, Inc. v. MP3.com, Inc.*
    d. *A&M Records, Inc. v. Napster, Inc.*

C. Limitation on Licenses: Intellectual Property Misuse

1. Copyright misuse
2. Patent misuse.

3. Trademark and domain name misuse
4. Trade secrets licenses

D. Antitrust Law & Investigations of Microsoft

E. Microsoft settlement

F. Internet-related Antitrust Litigation

1. *United States v. Microsoft*
   a. Majority Opinion
   b. Increasing Returns to Scale and Network Externalities
   c. Judge Wald's Concurrence
2. *United States v. Microsoft (II)*
3. *Intergraph Corp. v. Intel Corp.*
4. *Kesmai Corp. v. America Online, Inc.*
   a. Claims
   b. Allegations
   c. Settlement
5. *Cyber Promotions, Inc. v. America Online, Inc.*
6. *GTE New Media Services, Inc. v. Ameritech Corp.*

VIII. TORT LIABILITY OF ONLINE SERVICE PROVIDERS

A. No Liability Where an Online Service Acts Like a Book Store, Newsstand or Television Network

1. *Cubby, Inc. v. CompuServe Inc.*
   a. Facts
   b. Holding
   c. Vicarious liability
2. *Stern v. Delphi Internet Services Corp.*
   a. Facts
   b. Analogy to a television network

B. *Stratton Oakmont v. Prodigy Services, Inc.*

1. Facts
2. Prodigy was held to be a "publisher"
3. Cubby distinguished
4. "Board Leader" an agent of Prodigy
5. Policy implications
6. Appeal
7. Settlement/motion for reargument denied.
   a. Settlement
   b. December 1995 Opinion

C. The Telecommunications Act of 1996

1. *Stratton Oakmont* overruled
2. Policy objectives
3. Effect of the law

D. The Scope of Preemption of State Claims

1. *Zeran v. America Online, Inc.*
   a. Facts
   b. Zeran's Suit
   c. Holding
   d. Criticism
   e. Post-Zeran case law
2. Broad preemption of state claims and remedies.
   a. Expansive definition of affected parties

b. Impact
3. Immunity extends to third party (but not original) content
4. Web host not a content provider

E. Bulletin Board Postings Held Not to Be Periodicals, *It's In The Cards, Inc. v. Fuschetto*

1. Facts
2. Holding
3. A plea for legislative action

F. Tort Liability for Computer Viruses

IX. EMAIL

A. What Mode of Communication Does Email Replace?

B. When Is Email Private?

1. Email sent from or received on a home computer via America Online
2. Judicial Email
3. U.S. Government and business records.
   a. U.S. Government Email
   b. Email may not be a business record.
   c. Employee email is discoverable

C. Encryption and Internet Security

1. Encryption.
2. Litigation over encryption export controls.
   a. *Karn v. Department of State*
   b. *Bernstein v. Department of State*
   c. *Junger v. Daley*
3. Current Export Regulations.
   a. 1999 ITAR regulations
   b. 1998 Financial Institution Export Guidelines
4. Other security measures.
   a. Digital signatures.
   b. Steganography

D. Email, Client Confidences and the Attorney-Client Privilege

1. Reasonable protection
2. Is the use of email reasonable?
   a. Interception is unlawful
   b. Internet security.
   c. Gateway security
   d. Internal security employed by lawyers and clients
   e. Is encryption required?
3. Case law
   a. Disclosure destroys privilege
   b. Inhouse communications.
4. Ethics Opinions.

E. An Employer's Right to Monitor Employee Email

1. *Bohach v. Reno*
2. *Smith v. Pillsbury Co.*
3. California state trial courts

F. Liability for Email Transmissions

1. Employer liability for employee email
2. Employee email as evidence of a crime

G. Challenging Email Anonymity Under the ECPA

H. Spoliation of Email Evidence

X. SPAMMING AND THE LAW OF JUNK EMAIL

A. Definition

B. Case Law
1. *America Online, Inc. v. Cyber Promotions, Inc.*
2. *CompuServe Incorporated v. Cyber Promotions, Inc.*
3. *Concentric Network Corp. v. Wallace*
4. *Hotmail Corp. v. Van Money Pie, Inc.*
5. *America Online, Inc. v. Prime Data Systems, Inc.*

C. Administrative Regulation

D. State Regulation
1. State Statutes
2. Litigation

XI. PRIVACY LAWS AFFECTING THE CONDUCT OF ELECTRONIC COMMERCE

A. Overview

B. The EU Privacy Directive
1. Overview
2. Consent or Necessity
    a. Consent must be "unambiguously given," specific and informed
    b. Necessity
    c. Free speech
    d. Special categories
    e. Exemptions
3. Data Quality
4. Mandatory Disclosures
5. The Rights to Access Data and Object to its Processing
6. Confidentiality and Security
7. Transfer of Personal Data to Third Countries

C. The U.S. Response to the EU Privacy Directive
1. Self-regulation
2. Technology
3. U.S. Dept. of Commerce Safe Harbor Principles

D. U.S. Constitution
1. Privacy rights under the U.S. Constitution
2. The Fourth Amendment

E. The California Constitutional Right to Privacy
1. Personal data
2. Not Limited to Government Conduct.
3. Private Cause of Action.

F. Common Law

G. Statutes Protecting Privacy Rights
1. The Fair Credit Reporting Act
2. The Electronic Funds Transfer Act

3. The Child Online Protection Act
4. The Computer Fraud and Abuse Act
5. The Electronic Communications Privacy Act

H. FTC Privacy Guidelines for Fair Information Practices in Consumer Transactions

I. In re: GeoCities

1. FTC Allegations
2. Consent Judgment

J. Federal Regulatory Jurisdiction

1. Opt-in vs. opt-out procedures
2. The Commerce Clause
3. First Amendment Limitations

XII. OBSCENITY AND FREE SPEECH

A. Child Pornography

1. Distribution and possession illegal
2. Reporting requirement
3. Morphing and virtual child pornography
    a. Child Pornography Prevention Act of 1996
    b. Affirmative Defense
    c. Split in the Circuits

B. Interstate Transportation of Obscene Material

1. Transportation and distribution
2. *United States v. Maxwell*
3. *United States v. Chapman*
4. *United States v. Thomas*

C. The Communications Decency Act: Indecent and Patently Offensive Communications Directed at Minors

1. Vagueness
2. Breadth
3. Justice O'Connor's Zoning Analysis

D. The Child Online Protection Act: Commercial Speech Deemed "Harmful to Minors"

1. Harmful to minors
2. ISP Examption
3. Legal Challenge

E. Screening Software

F. State Regulation of the Internet

1. *American Library Association v. Pataki*
2. *ACLU v. Miller*
3. *Urofsky v. Gilmore*
4. *ACLU v. Johnson*

G. International Regulation of Offensive Material.

1. Germany
2. Singapore
3. The P.R.C.

XIII. INTERNET CRIMES

A. Criminal Copyright Infringement

B. Fraud and Abuse Act of 1986
1. 18 U.S.C. § 1030(a)(5)(A)
2. *United States v. Morris*

C. Threats Transmitted Via Email
1. *United States v. Baker*
   a. Indictment quashed.
   b. Threats too remote
2. Stalking laws

D. Trade Secrets

E. The National Stolen Property Act
1. Electronic theft covered by the act: *United States v. Riggs*
   a. Facts
   b. Conviction
   c. First Amendment defense rejected
2. Electronic theft not covered by the Act: *United States v. Brown*
   a. Holding
   b. Riggs analysis rejected

F. Wire Fraud

G. Civil Remedies for Unlawful Seizures, *Steve Jackson Games, Inc. v. U.S. Secret Service*
1. Facts
2. The Federal Wiretap Act
3. The Privacy Protection Act 136
4. Stored Wire and Electronic Communications 136 H. Use of the Internet for Law Enforcement

XIV. JURISDICTION

A. Personal Jurisdiction
1. Constitutional Test
2. Contracts
   a. *CompuServe, Inc. v. Patterson*
   b. *Hall v. LaRonde*
3. Operation of a website
   a. Early decisions
   b. Other courts
   c. *Bensusan Restaurant Corp. v. King*
   d. *Cybersell, Inc. v. Cybersell, Inc.*
   e. *Panavision Int'l, L.P. v. Toeppen*

B. U.S. Customs Law

C. Criminal Law

D. Attorney Advertising
1. Texas
2. Florida
3. North Carolina

E. Tax Law in Cyberspace
1. The Internet Tax Freedom Act.
   a. Moratorium
   b. Exclusions
   c. Exemption

2. Tax compliance

F. International Government Regulation of the Internet

1. Canada
2. EEC
3. Australia (with links to other international reports)

XV. UPDATE INFORMATION AND NEW CASE LAW

IAN C. BALLON is a partner who splits his time between the Palo Alto and Los Angeles offices of Manatt, Phelps & Phillips, LLP, where he concentrates on e-commerce, new media and intellectual property litigation, licensing and strategic counseling. Mr. Ballon is the author of the multi-volume legal treatise, *E-Commerce and Internet Law: Forms-Text-Cases,* published by Glasser LegalWorks (1-800-308-1700). He also co-chairs the Intellectual Property Working Group of the American Bar Association's International Cyberspace Jurisdiction Project. In 1999, he was named one of the top 20 California lawyers under age 40 by *California Law Business* magazine.

A frequent speaker and writer on Internet law, Mr. Ballon serves on the editorial boards of *The Cyberspace Lawyer, E-Commerce Law Report, The Journal of Internet Law, Privacy and Information Law Report and Intellectual Property Lawcast.* He is also the author of a number of articles, including "Spoliation of E-mail Evidence: Proposed Intranet Policies and A Framework For Analysis," The Cyberspace Lawyer, Mar. 1999; "Third Party Liability Under the Digital Millennium Copyright Act: New Liability Limitations and More Litigation for ISPs" (with Keith Kupferschmid), *The Cyberspace Lawyer,* Nov. 1998; "How Companies Can Reduce The Costs and Risks Associated With Electronic Discovery," *The Computer Lawyer*, July 1998; "Third Party Liability for Online Defamation Under the Telecommunications Act of 1996: Why the Fourth Circuit's Ruling in *Zeran v. America Online, Inc*. Is Wrong," *Journal of Internet Law,* Mar. 1998; "The Internet Applications of the Inevitable Disclosure Doctrine," *The Cyberspace Lawyer,* Feb. 1998; "Pinning the Blame in Cyberspace: Towards A Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet," 28 *Hastings Journal of Communications and Entertainment Law* 729 (1996); "The Internet Applications of the Economic Espionage Act of 1996," *The Cyberspace Lawyer,* Mar. 1997; "Strategies to Reduce Internet Liability," *Business Law News,* Fall 1996; "*dispute.com*: The Next Generation of Domain Name Litigation," *Intellectual Property,* Summer, 1996; "Court's Ambivalent Lotus Ruling Still Provides Valuable Insight," *The Computer Law Strategist,* Feb. 1996, at 1; and "Determining Fair Use in Cyberspace," L.A. Daily Journal, Sept. 6, 1995.

Mr. Ballon received an LLM in International and Comparative Law (with an emphasis on international protection of intellectual property) from Georgetown University Law Center and received his JD in 1986 from George Washington University, where he was the Articles Editor of The *George Washington Journal of International Law and Economics.* He received his BA in economics and political science from Tufts University.

He may be contacted at **iballon@manatt.com**.

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

I. DEFINITIONS AND CONCEPTS

Cyberspace: A term coined by William Gibson in the early 1980s in the short story "Burning Chrome." William Gibson, "Burning Chrome" in Burning Chrome (1987). In his subsequent science fiction novel "Neuromancer," Gibson prophesized a "virtual reality" generated by computers in which people could interact, conduct business and entertain themselves. William Gibson, Neuromancer 55 (1984); Flex H. Kent & Lawrence M. Hertz, "Establishing a Foothold in Cyberspace," N.Y.L.J., Apr. 21, 1995, at 3. The Information Superhighway: A popular term used especially during the 1992 presidential campaign to describe a vision of a world wide communications network, akin to what the Internet is today.

The Internet: The world's largest computer network, connecting other computer networks and users. The Internet developed from a project conceived in 1966 by Bob Taylor, the director of the computer research program at the U.S. Department of Defense's Advanced Research Project Agency ("ARPA") to link computers together so that research facilities could pool their resources. The first node of what initially became known as Arpanet was installed at UCLA in 1969. Cisler, "The Creators," Wired, Dec. 1994, at 153. Today, the Internet connects over 19.5 million individual servers, or host computers, around the world. Eryn Brown, "The Net Is Growing Fast! Or Maybe It's Slowing! Or Both!," Fortune, Oct. 13, 1997. Each server is linked to and accessible from any other point on the Internet over a matrix of interconnected networks. By means of standard protocols and application-specific client-server software such as ftp, Gopher, World Wide Web ("WWW"), Usenet News and Internet Relay Chat, Internet servers provide to over 30,000,000 Internet users many of the same services offered by more traditional bulletin board services. Maureen A. O'Rourke, "Copyright Liability of Computer Bulletin Board Operators for Infringement by Subscribers," 1 B.U.J. Sci. & Tech. 6 (1995). The Internet is a cooperative venture not owned by any single entity or government.

Internet 2: A faster computer network being developed by 112 universities that will allow for enhanced voice, video and data capabilities. Internet 2 is intended to address researchers' frustrations at being unable to obtain files as quickly as needed because of the volume of business and residential traffic over the Internet. Internet 2 should improve computer connections and allow for more important traffic to be sent ahead of low priority communications (which is not possible over the Internet). AP, "Internet 2 to be Unveiled this Week," Oct. 5, 1997.

Home Page: The first (and central) page on a website.

Web Page: Websites are comprised of multiple "pages" (which may be shorter or longer than actual paper pages of information). As explained by one court, a web page is a computer data file on a host operating a web server within a given domain name. When the web server receives an inquiry from the Internet, it returns the web page data in the file to the computer making the inquiry. The web page may comprise a single line or multiple pages of information and may include any message, name, word, sound or picture, or combination of such elements.

Intermatic Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996). *See website, home page.*

Website: A website is an electronic location on the World Wide Web that may contain text, graphics, visual images or sound. Websites are created using HTML (hypertext markup language), which is interoperable with all existing software platforms. A court in the Eastern District of Missouri described the process of accessing a website as follows:

> Any Internet user can access any website, of which there are presumably hundreds of thousands, by entering into the computer the Internet address they are seeking. Internet users can also perform searches on the Internet to find websites within targeted areas of interest. Via telephone lines, the user is connected to the website, and the user can obtain any information that has been posted at the website for the user. The user can also interact with and send messages to that website. Upon connecting to a website, the information is transmitted electronically to the user's computer and quickly appears on the user's screen. This transmitted information can easily be downloaded to a disk or sent to a printer.

Maritz, Inc. v. CyberGold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996).

BBS: Bulletin board service. A BBS allows subscribers to upload and download data and post messages. A BBS typically caters to a particular audience.

A Newsgroup: "[A]n electronic discussion group, serving as a bulletin board for users to post universally accessible messages, and to read and reply to those from others." *Religious Technology Center v. F.A.C.T.Net, Inc.,* 901 F. Supp. 1519 (D. Colo. 1995).

Usenet: The Usenet has been described as

> a worldwide community of electronic BBSs that is closely associated with the Internet and with the Internet community. The messages in Usenet are organized into thousands of topical groups, or "Newsgroups" . . . . As a Usenet user, you read and contribute ("post") to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings and from other sites. Usenet traffic typically consists of as much as 30 to 50 Mbytes of messages per day. Usenet is read and contributed to on a daily basis by a total population of millions of people. . . . There is no specific network that is the Usenet. Usenet traffic flows over a wide range of networks, including the Internet and dial-up phone links.

Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1365 (N.D. Cal. 1995), *citing* Daniel P. Dern, The Internet Guide for New Users 196-97 (1994).

Database: A database is a compilation of information stored in digital form.

Online Service/Content Provider: A company that maintains databases and potentially other services, which may be accessed remotely by subscribers using a personal computer and a modem. Examples of online content providers are Mead Data's LEXIS/NEXIS service, which contains information databases, and CompuServe, America Online and Prodigy, which offer a wide array of services, including online conferences and discussion groups similar to a traditional BBSs, some access to the Internet, information services and entertainment.

Internet Access Provider: A company that provides subscribers with access to the Internet (but not necessarily content). For example, Netcom is an access provider. CompuServe, by contrast, provides its subscribers with access to the Internet but is also a content provider.

Download: The process of transferring information from a BBS or the Internet to a user's own computer. For example, photographic images taken by the space shuttle and available in digital form online may be downloaded to a user's own personal computer.

Upload: The process of transferring information from a user's own computer to a BBS or Internet site.

Netiquette: Internet etiquette. "[T]he informal rules and customs that have developed on the Internet . . ." *Religious Technology Center v. Netcom On-Line Communication Service, Inc.,* 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

Spamming: The practice of sending thousands - or even millions - of the same message to Internet users either through Usenet groups or email, typically hawking a client's product or agenda. The term is taken from a Monty Python's Flying Circus skit. S. Garfinkel, "The King of Spam," *San Jose Mercury News,* Oct. 24, 1995, at 1A. One of the most famous examples of spamming occurred in 1994 when a pair of immigration lawyers broadcast an advertisement to approximately 5,000 newsgroups. The spammers received over 30,000 replies, mostly in the form of "hate email." M. Hansen, "Lawyers' Internet Ad Angers Users," A.B.A.J., July 1994, at 26.

Flaming: The practice of sending strident or offensive email messages.

Firewall: A firewall is a collection of components or a system that is placed between two computer networks (through which all traffic into or out of a network must pass), which prevents unauthorized access to a network and is itself immune to penetration. National Computer Security Association, NCSA Firewall Policy Guide 5 (1996), *citing* William R. Cheswick & Steven M. Bellovin, Firewalls and Internet Security (1994). A firewall should be established between a company's network and the Internet, and potentially also within a company's wide area network.

Agent Software: Intelligent software. Also known as off-line software, robots, bots or droids.

Banners: Online advertisements typically flashed across the top (or a segment) of the screen on a website.

Bookmark: A bookmark saves a web address to memory so that it may be easily recalled at a later time without having to either type in a long, cumbersome address to locate a desired site, or use a search engine to locate it again. Unlike a book mark used to save a place in a book, a web bookmark actually stores the address so it can be recalled at a later time. "A bookmark is used to help users return quickly to web pages that he or she visits often." *Malarkey-Taylor Associates, Inc. v. Cellular Telecommunications Industry Association,* 929 F. Supp. 473, 477 n.3 (D.D.C. 1996).

Hyperlinks: Underlined portions of text on a website that will allow a visitor to the site, by clicking on the highlighted text, to be connected to a different site. As explained by one court:

> A hyperlink is a link from one site on the Internet to a second site on the Internet. "Clicking" on a designated space on the initial page that references the subsequent site by a picture, by some highlighted text or by some other indication will take a person viewing the initial web page to a second page. In addition to their use in indexes [sic], hyperlinks are commonly placed on existing web pages, thus allowing Internet users to move from web page to web page at the click of a button, without having to type in URLs.

Intermatic Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996).

Intranet: An internal network cordoned off from the public through firewalls that uses the infrastructure and standards of the Internet and World Wide Web. See "Here Comes the Intranet," *Bus. Week*, Feb. 26, 1996, at 76.

Extranet: An extranet is a network linking portions of (or entire) intranets, and exists behind firewalls. Companies that work closely, such as manufacturers and suppliers or joint development partners, may want to share information with each other, but not third parties, and therefore link

their intranets.

Push Technology: Technology that allows information to be automatically collected and "pushed," or delivered directly to a user, who might otherwise have had to affirmatively search for it, or "pull" the information from a database, intranet or the Internet. *See also Off-Line Software, Agent Software.*

TCP/IP: Transmission Control Protocol and Internet Protocol. TCP/IP is used as a shorthand reference for more than 100 protocols used to connect computers and networks and move information over the Internet. Harley Hahn, The Internet Complete Reference 20-21 (2d ed. 1996). Information sent over the Internet is broken into packets that are separately routed and then reassembled at an intended location. TCP is the protocol used to divide data into packets, which are then marked with a sequence number, the recipient's address and the address of the sender. Packets are transmitted over the Internet by IP, which directs the packets in the most efficient route, automatically rerouting packets when particular links cannot be transversed or are congested. A router determines the actual direction taken by a given packet. Therefore, the various packets that comprise a message may be sent by different routes over different computer systems located in different states before reaching their intended destination where they are reassembled according to TCP protocol. Harley Hahn, The Internet Complete Reference 21 (2d ed. 1996).

URL (pronounced "U.R.L.," not "earl"): Uniform Resource Locator. The address for a website.

The Significance of Digital Technology: Information, sound and video stored in digital form (in a series of 1s and 0s known as binary code) may be easily manipulated - transmitted electronically (including over the Internet), combined with other information stored in digital media and reproduced *exactly.* Unlike information stored in analog form, digital form data may be copied, and the copies copied, without any degradation in quality.

Ease of Infringement: Since information in digital form can be easily manipulated, it also can be easily infringed. For example, Macromedia, Inc., a software developer, brought suit alleging that individual America Online subscribers (using 67 pseudonyms) infringed its copyrights by copying and distributing its works via America Online's Email system. *Macromedia, Inc. v. VRHacker,* Case No. C95-1261 (N.D. Cal. Filed Apr. 13, 1995), as reported in CyberLex (May 15, 1995). In 1994, it was estimated that software pirated from online services accounted for about one-third of the $2.2 billion lost each year by the U.S. software industry. Adam S. Bauman, "The Pirates of the Internet," L.A. Times, Nov. 3, 1994, at A1. This problem is likely to increase as more people come online.

Speed of Delivery: With a single key stroke or click of a mouse, information (including text, sound, visual images and other data in digital form) can be sent to hundreds of people around the world via email. The speed of delivery is dependent upon the software, hardware and service used by the sender and recipient. Depending on the configurations used, information can be transmitted across the country in a matter of minutes.

International Boundaries Dissolve over the Internet: The international scope of cyberspace has made it more difficult to enforce local laws. For example, when an Ontario judge ordered a news blackout on coverage of the Homulka murder trial, which, consistent with Canadian law, resulted in *Wired* magazine's April 1994 issue being censored in Canada, *Wired* magazine posted a press release at its website, listing Internet addresses where the censored articles and other information on the trial could be obtained by Canadian residents. *See* Press Release, "Cyberspace Cannot Be Censored," *Wired* Online Service. Similarly, Canadian and French laws imposing blackouts on the reporting of poll results immediately prior to national elections were undermined in 1997 by individuals who established off-shore websites to report such information.

By contrast, the enforcement of local laws relating to the Internet may have international ramifications. For example, in late 1995, CompuServe announced that, in response to a claim

from federal prosecutors in Germany that the pornographic content of certain Internet newsgroups violated German law, CompuServe would block its subscribers from accessing as many as 250 Internet newsgroups from its worldwide network because it could not block access solely to its German subscribers. "CompuServe Blocks Access to Some Internet Porn," The Daily Record, Dec. 29, 1995, at 1. Enforcement of German hate crime laws also underscores the overlapping nature of jurisdiction in cyberspace, where conduct in one country may subject parties to liability elsewhere. The prosecutor's office in Mannheim, Germany launched an investigation of CompuServe and Deutsche Telekom's T-Online service for inciting racial hatred because these online services, as Internet providers, allowed Germans to access a website run by a neo-Nazi extremist in Canada who used the Internet to distribute anti-Semitic propaganda. Edupage, Jan. 28, 1996, *citing* The Wall Street Journal, Jan. 26, 1996, at B2. In April 1997, the general manager of CompuServe Deutschland was indicted for trafficking in pornography and neo-Nazi propaganda (accessible to CompuServe's German subscribers over the Internet). Ultimately, the Canadian in whose name the anti-Semitic site operated argued that he could not be prosecuted under Canadian law because the website in question was actually based in California, and operated without his consent.

Feelings of Anonymity: Some Internet users develop a false sense of anonymity by moving through virtual communities using minimal identification that does not reveal a person's true name, home address or even sex. As a result, people may act without the constraints they might feel in face-to-face interactions. For example, certain netizens feel unconstrained to "flame" other users (or post personal attacks on a BBS or online conference), while in person they might not be willing to be so confrontational. Similarly, some people seem to feel less hesitant about downloading and uploading proprietary software and other data (especially given the volume of public domain information and data and shareware that may be freely downloaded), even though they would not think of stealing a box of prepackaged software off the shelf of a commercial software vendor. Although a user can move through the Internet with relative anonymity, his actions can be traced, as shown by the apprehension in 1995 of hacker Kevin Mitnick. *See, e.g.,* Tsutomu Shimomura & John Markoff, Takedown (Hyperion 1996). In addition, new technologies are being developed which may make tracing people online even easier.

The Convergence of the Software and Entertainment Industries: Digital technology has made possible the combination of different media that once were distinct. One of the results is a convergence of the software and entertainment industries. Video games, CD-ROMs and computer graphics used in movies are merely some examples of this trend. More recently, the Rolling Stones and other groups have broadcast concerts over the Internet. As computers become more powerful, this trend is bound to continue. MSNBC and Microsoft's acquisition of WebTV also exemplify the convergence of software and entertainment.

The Convergence of the Telecommunications, Cable and Information Technology Industries: Computer networks typically are linked to the Internet by telephone lines and modems. New technologies, including faster modems, data compression and new data transmission media will increase the speed with which information may be transmitted between computers. Since 1995, local telephone companies have offered customers access to Integrated Services Digital Network (ISDN) communication lines that can transmit data at 128 kilobits per second (compared to 56 kilobits, which is the fastest modem commonly available for home use), without any of the transmission errors common on analog connections. Marcelo Rodriguez, "An Accelerator for the Net," San Jose Mercury News, Oct. 29, 1995, at E-1. Asynchronous digital subscriber lines (ADSL) and T-1 lines can deliver information at even greater speeds. Competing with telephone companies for communications business will be cable companies, whose coaxial cables can transmit data at much faster speeds than traditional phone lines. Faster delivery of information and more powerful computers have made possible Internet telephony and videoconferencing and will enable new uses of the Internet in the years to come. The passage of the Telecommunications Act of 1996 has only accelerated the convergence of the cable, telephone and computer industries.

The Convergence of Internet Companies: The previously distinct roles served by companies

which offered different Internet services now overlap. Search engines, browsers, online services and even computer operating systems are beginning to look more like one another.

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

II. COPYRIGHT PROTECTION IN CYBERSPACE

A. Statutory Background

1. U.S. copyright law protects expression, but not underlying ideas.

2. Copyright protection extends to:

a. Original works of authorship

b. Fixed in a tangible medium of expression. 17 U.S.C. § 102(a).

(1) **Software** is deemed to be "fixed in a tangible medium" even when not stored on disk. *MAI Systems Corp. v. Peak Computer, Inc.,* 991 F.2d 511 (9th Cir. 1993) (turning on a computer, which causes the operating system to be loaded from permanent storage to the computer's random access memory (RAM), was held to constitute copyright infringement where the person turning on the computer was not licensed to use the operating system), *cert. dismissed,* 510 U.S. 1033 (1994); *see also Triad Systems Corp. v. Southeastern Express Co.,* 64 F.3d 1330 (9th Cir. 1995), cert. denied, 516 U.S. 1145 (1996); *Advanced Computer Services v. MAI Systems Corp.,* 845 F. Supp. 356 (E.D. Va. 1994) (same holding). In *MAI Systems Corp.,* the Ninth Circuit wrote that "[t]he representation created in the RAM 'is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.'" 991 F.2d at 518.

(2) **Usenet newsgroup postings.** In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361 (N.D. Cal. 1995), Usenet postings of copyrighted works were held to create "copies" under *MAI Systems Corp. v. Peak Computer, Inc., supra,* (1) when automatically (and briefly) stored on a BBS computer and then (2) when automatically copied to an Internet access provider's computer and then (3) when automatically copied onto other computers on the Usenet. See infra § II(F)(7).

(3) **Browsing.** When a user browses the Internet, the act

of browsing causes a copy of the digital information viewed on the screen temporarily to be made in the user's computer screen memory. Under *MAI Systems Corp. v. Peak Computer, Inc., supra,* a copy is fixed when information is temporarily placed in RAM, including screen RAM. *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361, 1378 n.25 (N.D. Cal. 1995); see infra § II(F)(7).

(4) **Interactive works** are also deemed to be "fixed in a tangible medium," even though the sequence of action can be altered by each individual user. *See Atari Games Corp. v. Oman,* 888 F.2d 878, 884 (D.C. Cir. 1989).

3. Copyright protection may be obtained for:

a. Literary works. As a result of the recommendations of the CONTU commission, Congress, in 1980, expressly amended the 1976 Copyright Act to provide that software be treated as a "literary work." *See Apple Computer, Inc. v. Formula Int'l Inc.,* 725 F.2d 521, 524-25 (9th Cir. 1984).

b. Musical works, including any accompanying words.

c. Dramatic works, including any accompanying music.

d. Pantomimes and choreographic works.

e. Pictorial, graphic and sculptural works.

f. Motion pictures and other audiovisual works. Screen displays, or the user-interface of a computer program, may be entitled to protection as an audiovisual work. *See, e.g., Computer Associates Int'l, Inc. v. Altai, Inc.,* 982 F.2d 693, 703 (2d Cir. 1992).

g. Sound recordings.

h. Architectural works. 17 U.S.C. § 102(a).

4. Copyright protection does *not* extend to any idea, procedure, process, system, method of operation, concept, principle or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work. 17 U.S.C. § 102(b).

5. **Exclusive rights in copyrighted works**. A copyright grants the owner the exclusive right to do and authorize any of the following (subject to the first sale doctrine codified at 17 U.S.C. § 109(a), *infra* § VII(A)(1)):

a. to reproduce the copyrighted work in copies or phonorecords;

b. to prepare derivative works based upon the copyrighted work;

c. to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

d. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;

e. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and

f. in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission. 17 U.S.C. § 106.

6. **Exception to a copyright owner's exclusive rights: archival or back-up copies of software and temporary copies created for maintenance or repair.** 17 U.S.C. § 117 creates an exception to the exclusive rights granted a copyright owner under 17 U.S.C. § 106 for back-up copies of software programs. Pursuant to a 1998 amendment to the Copyright Act, a narrow exception also exists for temporary copies created "solely by virtue of the activation of a machine that lawfully contains an authorized copy . . . for purposes only of maintenance or repair of that machine . . . ."

B. Derivative Works and Multimedia Clearance

1. **Definition.** A "multimedia work" generally refers to a work that incorporates more than one media form, such as film, video, text, audio, photographs, graphics and/or animation, and which typically is stored in digital form.

2. **Multimedia works often are "derivative works".** As a result of digital technology, it is today relatively easy to cut and past sound, visual images, text and software applications to create new "works." These works generally would be characterized as "derivative works," because they are based on preexisting works. 17 U.S.C. § 101. Copyright protection in a derivative work or compilation extends only to the material contributed by the author of such work, and does not grant rights in the preexisting works included in the new work. 17 U.S.C. § 103.

3. **Clearance.** With multimedia works, it is important to ensure that permission to use each aspect of the work has been obtained. The rights to each prior work incorporated in a derivative multimedia work (i.e., text, motion pictures, software) typically are owned by different entities. In addition, since all of the rights granted by a copyright may be separately licensed, different entities may have exclusive licenses to different forms of the same work (i.e., book rights, motion picture rights, etc.). Further, even an exclusive licensee may not have rights which would extend to a new, multimedia application. Clearance issues therefore can be quite complex and, if not properly addressed, lead to litigation. Clearance problems are likely to become more pronounced, and spawn more litigation, as more people gain access to online services and the Internet, more data becomes available online and users increasingly are able to create sophisticated multimedia applications simply by cutting and pasting works accessible from their home or work computer.

4. **Digital technology challenges traditional copyright law.** Professor Pamela Samuelson and Robert Glushko have identified several characteristics of works in digital form that are likely to change the contours of copyright law, including: (1) the ease with which such works can be replicated and the ease with which they can be transmitted and accessed by multiple users "would seem to create strong incentives for copyright industries to move away from their traditional focus of the sale of copies, and toward greater control over uses of protected works"; (2) the ease with which digital works can be manipulated and modified creates new benefits and problems since copyright law is more geared toward dealing with works that are permanently fixed; (3) the breakdown among copyright distinctions among different kinds of works when they are in digital form suggests that the eight categories of protected works (*supra* § II(A)(3)), each of which has somewhat varying degrees of

protection, need to be revised; and (4) digital works allow new kinds of search and linking activities to be achieved, giving rise to hybrid multimedia works, which the authors characterize as "new classes of protected intellectual property products, including hypertext." Symposium, "Electronic Communications and Legal Change: Intellectual Property Rights for Digital Library and Hypertext Publishing Systems," 6 Harv. J.L. & Tech. 237, 237-40 (1993). An example that the authors provide is of a hypertext version of Mozart's "Magic Flute" that contains the music, the libretto, textual commentary, pictures of Mozart and other media, which under traditional copyright analysis must be labeled a "literary work," a "musical work," a "sound recording," a "pictorial work," or an "audio visual work," even though the work in fact is all of these things. *Id.* at 240.

C. Software Infringement

1. **What is protectable?** The level of creativity required for a work to qualify for copyright protection is extremely low. As explained by the U.S. Supreme Court, "the requisite level of creativity is low; even a slight amount will suffice." *Feist Publications, Inc. v. Rural Telephone Service Co.,* 499 U.S. 340, 345 (1991). Despite this low standard, many "minimally creative" or functional aspects of computer programs are not entitled to copyright protection. Although the law in this area is still evolving, and varies in certain respects in the different federal circuit courts, the following are examples of aspects of software programs that may not be entitled to copyright protection:

a. **Menu command hierarchies.** *See Lotus Development Corp. v. Borland Int'l, Inc.,* 49 F.3d 807 (1st Cir. 1995), *aff'd mem.,* 516 U.S. 233 (1996) (4-4 decision). *But see Autoskill Inc. v. National Educational Support Systems, Inc.,* 994 F.2d 1476 (10th Cir.), *cert. denied,* 510 U.S. 916 (1993) (*rejecting* the defendant's argument that the keying procedure used in a computer program designed to test and train students with learning deficiencies was an uncopyrightable "procedure" or "method of operation"); *see also Lotus v. Borland,* 49 F.3d at 819-21 (Boudin, J. concurring) (emphasizing that Lotus' menu commands presented a particularly unattractive case for copyright protection because they "are largely for standard procedures that Lotus did not invent and are common words that Lotus cannot monopolize . . .").

b. **Icons.** *Apple Computer, Inc. v. Microsoft Corp.,* 35 F.3d 1435, 1443-44 (9th Cir. 1994), *cert. denied,* 513 U.S. 1184 (1995) (holding unprotectable Apple's "iconic representation of familiar objects from the office environment" and "the manipulation of icons to convey instructions and to control operation of the computer").

c. **Use of windows** to display multiple images on the computer screen and to facilitate user interaction with the information contained in the windows. *Id.*

d. **Use of menus** to store information or computer functions in a place that is convenient to reach, but saves screen space for other images. *Id.*

e. **Opening and closing of objects** as a means of retrieving, transferring and storing information. *Id.*

f. A **computer animated key pad.** *Mitek Holdings, Inc. v. ARCE Engineering Co.,* 864 F. Supp. 1568, 1581 (S.D. Fla. 1994), *aff'd,* 89

F.3d 1548 (11th Cir. 1996).

g. **Constants.** Constants are the invariable integers that comprise part of the formulas used to perform the calculations in certain programs. In *Gates Rubber Co. v. Bando Chemical Industries, Ltd.,* 9 F.3d 823 (10th Cir. 1993), the constants represented scientific observations of physical relationships concerning the load that a particular belt can carry around certain sized gears at certain speeds given the number of other variables. These constants were deemed to be unprotectable since the relationships shown by the programs "are not invented or created; they already exist and are merely observed, discovered and recorded." *Id.* at 842-43.

h. **Databases.** Copyright protection for a database, as a compilation, does not extend to preexisting works stored in the database. See 17 U.S.C. § 103. Since purely factual compilations (such as phone books) are not entitled to copyright protection, *Feist Publications, Inc. v. Rural Telephone Service Co.,* 499 U.S. 340 (1992), databases are likely to receive little or no protection under copyright law*. But see CCC Information Services, Inc. v. MacLean Hunter Market Reports, Inc.,* 44 F.3d 61 (2d Cir. 1994) (finding a factual compilation entitled to copyright protection), *cert. denied,* 516 U.S. 817 (1995).

i. **Input/output formulas.**

(1) In *Engineering Dynamics, Inc. v. Structural Software, Inc.,* 26 F.3d 1335, 1343-44, 1346 (1994), *modified and reh'g denied,* 46 F.3d 408 (5th Cir. 1995), the Fifth Circuit reversed a district court determination that input and output formulas in an applications program designed to solve structural engineering problems were unprotectable. The I/O formulas in that case consisted of a series of words and a framework of instructions that acted as a prompt for the insertion of relevant data.

(2) The precedential value of **Engineering Dynamics, Inc. v. Structural Software, Inc.** is uncertain. The Fifth Circuit relied heavily on Judge Robert Keeton's decisions in *Lotus Development Corp. v. Paperback Software Int'l.,* 740 F. Supp. 37 (D. Mass. 1990) and *Lotus Development Corp. v. Borland Int'l, Inc.,* 831 F. Supp. 223, 231 (D. Mass. 1993), *rev'd,* 49 F.3d 807 (1st Cir. 1995), *aff'd mem.,* 516 U.S. 233 (1996) (4-4 decision), and in particular on Judge Keeton's finding (which was subsequently reversed by the First Circuit) that Lotus' menu command structure was entitled to copyright protection. The Fifth Circuit's holding that "the creativity inherent in [plaintiff's] program is proved by the existence of other, dissimilar structural engineering programs available in the market," is directly contradicted by the First Circuit's holding that creativity cannot transform a "method of operation" into protectable expression in *Lotus Development Corp. v. Borland Int'l, Inc.,* 49 F.3d 807, 818 (1st Cir. 1995) ("the fact that there may be many different ways to operate a computer program, or even many different ways to operate a computer program using a set of hierarchically arranged command

terms, does not make the actual method of operation chosen copyrightable . . ."), *aff'd mem.*, 516 U.S. 233 (1996) (4-4 decision).

j. **Threshold values**. In *Compaq Computer Corp. v. Procom Technology Inc.,* 908 F. Supp. 1409 (S.D. Tex. 1995), the court held that Compaq's threshold values (or the value of specific parameters selected by Compaq to trigger a prefailure warning in certain of Compaq's hard disk drives; when reached, Compaq would replace the drive if it was still under warranty) were protectable, although the order in which the threshold values appear on a hard disk drive constitute unprotectable *scenes a faire.*

The court held that the threshold values were protectable because in designing its prefailure warning system, Compaq determined both the number and particular parameters it would monitor, and the appropriate threshold value for each of the five parameters ultimately selected (which involved both engineering *and* business-related judgments).

2. **Audiovisual works: screen displays and interfaces.**

a. Screen displays may be protectable as audiovisual works even where the underlying code is not protectable as a literary work. *Computer Associates Int'l, Inc. v. Altai, Inc.,* 982 F.2d 693, 703 (2d Cir. 1992) (citing older cases).

b. Interfaces protected as audiovisual works should be analyzed under the same test for evaluating protectability and infringement as software programs registered as literary works. *Apple Computer, Inc. v. Microsoft Corp.,* 35 F.3d 1435, 1445 (9th Cir. 1994), *cert. denied,* 513 U.S. 1184 (1995).

3. **What constitutes infringement?**

a. **Elements.** To prevail in an infringement action, a copyright owner must prove (1) ownership of a valid copyright, and (2) infringement by the defendant. *E.g., Data East USA, Inc. v. Epyx, Inc.,* 862 F.2d 204, 206 (9th Cir. 1988). Since direct evidence of copying often is unavailable, a plaintiff may show infringement by evidence that (a) the defendant had access to plaintiff's work, and (b) the two works are substantially similar. *E.g., Brown Bag Software v. Symantec Corp.,* 960 F.2d 1465 (9th Cir.), *cert. denied*, 506 U.S. 869 (1992).

b. **Ownership.** A copyright registration certificate constitutes prima facie evidence of the validity of a copyright and the facts stated in the certificate, including the originality of the work and the ownership of the copyright. 17 U.S.C. § 410(c); *Service & Training, Inc. v. Data General Corp.,* 963 F.2d 680, 688 (4th Cir. 1992). By presenting prima facie evidence of the validity of its claims, the burden of proof shifts to the defendant to dispute the validity of plaintiff's copyrights. *E.g., Harris Market Research v. Marshall Marketing & Communications, Inc.,* 948 F.2d 1518, 1526 (10th Cir. 1991).

c. **Infringement by literal code copying**. Verbatim copying of object code or source code constitutes copyright infringement (assuming the portions of code copied include original, protectable elements). *E.g.,*

Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 702 (2d Cir. 1992); *Kepner-Tregoe, Inc. v. Leadership Software, Inc.,* 12 F.3d 527, 534 (5th Cir.), *cert. denied,* 513 U.S. 820 (1994). Since the level of creativity required for copyright protection is low (*supra* § II(C)(1)), direct evidence that a defendant copied substantial portions of a program generally will be sufficient to show copyright infringement.

d. **Infringement by non-literal copying/"look and feel" infringement.** Most of the battles over the scope of copyright protection for computer software have been fought in non-literal infringement cases, where the plaintiff alleges that the "look and feel" of a program (but not necessarily the literal code) have been copied.

(1) **Third Circuit:**

(a) The Third Circuit was the first to define the scope of copyright protection in cases of alleged non-literal infringement. In *Associates, Inc. v. Jaslow Dental Laboratory, Inc.,* 797 F.2d 1222 (3d Cir. 1986), *cert. denied,* 479 U.S. 1031 (1987), the Third Circuit adopted a broad view of the scope of copyright protection for computer software, holding that copyright protection extends beyond a program's literal code to its "structure, sequence and organization." Under the Third Circuit's test, as a practical matter, the "idea" of a program is defined very narrowly, and everything not necessary to the program's purpose or function is deemed to constitute protectable expression. 797 F.2d at 1236.

(b) Especially since the U.S. Supreme Court's rejection of the "sweat of the brow" doctrine in its 1991 decision in *Feist Publications, Inc. v. Rural Telephone Service Co.,* 499 U.S. 340, 361 (1991), the Third Circuit test has been severely criticized as taking an unduly broad view of the scope of copyright protection. *E.g., Computer Associates Int'l, Inc. v. Altai, Inc.,* 982 F.2d 693, 706 (2d Cir. 1992); *Sega Enterprises Ltd. v. Accolade, Inc.,* 977 F.2d 1510, 1525 (9th Cir. 1992); CMAX/Cleveland, Inc. v. UCR, Inc., 804 F. Supp. 337, 352 (M.D. Ga. 1992); *Micro Consulting, Inc. v. Zubeldia,* 813 F. Supp. 1514, 1528 (W.D. Ok. 1990), *aff'd mem.,* 959 F.2d 245 (10th Cir. 1992). *Whelan Associates,* however, has not been modified or overruled by the Third Circuit.

(2) **Second, Fifth, Ninth, Tenth and Eleventh Circuits:**

(a) Analytic Dissection/Abstraction - Filtration - Comparison. *E.g., Computer*

Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992); *Engineering Dynamics, Inc. v. Structural Software, Inc.,* 26 F.3d 1335 (1994), *modified and reh'g denied,* 46 F.3d 408 (5th Cir. 1995); *Brown Bag Software v. Symantec Corp.,* 960 F.2d 1465, 1472 (9th Cir.), cert. denied, 506 U.S. 869 (1992); *Gates Rubber Co. v. Bando Chemical Industries, Ltd.,* 9 F.3d 823 (10th Cir. 1993); *Bateman v. Mnemonics, Inc.,* 79 F.3d 1532 (llth Cir. 1996); *see also, e.g., Control Data Systems, Inc. v. Infoware, Inc.,* 903 F. Supp. 1316 (D. Minn. 1995) (applying abstraction - filtration - comparison).

(b) Under the *Altai* test, courts must first dissect the structure of the copyright owner's program to isolate each level of abstraction, beginning with protectable expression (typically object code) and ending with the unprotectable idea of the program (its ultimate function). The Second Circuit describe this first part of the test, known as "abstraction," as resembling "reverse engineering on a theoretical plane." Courts next must examine each component part of the program (at each level of abstraction) to filter out unprotectable aspects of the program, including expression not original to the author, aspects which constitute "the idea" of the program, expression necessarily incident to the idea, expression in the public domain and expression dictated by external factors (like the mechanical specifications of the hardware on which the program was designed to run, the need to make the program compatible with other programs and the demands of the industry served by the program). Finally, a court will be "left with a kernel, or possibly kernels, of creative expression" which would then be compared with the allegedly infringing program to determine whether protectable elements of the copyright owner's program have been infringed.

(3) **First Circuit:** the First Circuit declined to apply the majority *Altai* test in *Lotus Development Corp. v. Borland Int'l, Inc.,* 49 F.3d 807 (1st Cir. 1995), *aff'd mem.,* 516 U.S.. 233 (1996) (4-4 decision), holding that the application of the test in that case could actually be misleading. The First Circuit wrote that, in instructing courts to abstract the various levels of a software program, the test implicitly assumed that there was a

base level for each program that included copyrightable subject matter.

(4) For an analysis of the current state of the law governing nonliteral software infringement, *see* Ian C. Ballon, "Court's Ambivalent *Lotus* Ruling Still Provides Valuable Insight," The Computer Law Strategist, Feb. 1996, at 1.

e. **Infringement based on exceeding the scope of a license/ "virtual identicality" required in some instances.** In a true license, a licensor grants a licensee fewer rights than it is granted under patent or copyright law. A licensee who exceeds the scope of its license can be held liable for copyright infringement. *E.g., S.O.S., Inc. v. Payday, Inc.,* 886 F.2d 1081, 1087-89 (9th Cir. 1989). Where almost all of a work is comprised of elements licensed by the plaintiff, plaintiff must show virtual identicality, rather than merely substantial similarity, in order to prevail in a copyright infringement action. *E.g., Apple Computer, Inc. v. Microsoft Corp.,* 35 F.3d 1435, 1442 (9th Cir. 1994), *cert. denied,* 513 U.S. 1184 (1995).

f. **Infringement through unauthorized importation.** A plaintiff can establish infringement by evidence that, without the copyright owner's authorization, the defendant imported and then sold in the United States goods protected by a U.S. copyright. 17 U.S.C. § 602(a); *BMG Music v. Perez,* 952 F.2d 318, 319-20 (9th Cir. 1992), *cert. denied,* 505 U.S. 1206 (1992). It remains to be determined whether software protected by U.S. copyrights and downloaded in the United States from Internet sites "located" abroad, could be subject to section 602(a)'s import restrictions.

g. **Infringement via the Internet.** Internet users (unlike consumers who obtain software from traditional retail stores) are more likely to download programs and cut and paste portions of code into new programs. Although these acts of potential infringement involve literal code copying, "look and feel" cases will provide important guidance in determining which bits of code may be protectable because these cases define the outer contours of copyright protection for computer software.

D. Liability Under the Computer Software Rental Amendments Act

1. The Computer Software Rental Amendments Act prohibits any person "for the purposes of direct or indirect commercial advantage [to] dispose of, or authorize the disposal of . . ." a computer program acquired on or after 12/1/90 "by rental, lease or lending, or by any other act or practice in the nature of rental, lease or lending." 17 U.S.C. § 109(b)(1)(A).

2. *Central Point Software, Inc. v. Global Software & Accessories, Inc.,* 880 F. Supp. 957 (E.D.N.Y. 1995).

a. In perhaps the first case decided under the Computer Software Rental Amendments Act, Judge Leonard Wexler of the Eastern District of New York held that a computer software company's "sale" of software under a deferred billing plan amounted to the rental of software

prohibited by the Act.

b. **Deferred billing.** Under the defendant's deferred billing plan, customers paid a small "nonrefundable deposit" for the software and were not billed for the balance if they returned it within five days. Judge Wexler found that the transactions were tantamount to rentals, since (a) defendant's brochures advertised the "nonrefundable deposit," not the purchase price of software, (b) nearly 100% of the software was returned, (c) the deposits were comparable to rental fees, (d) the short term of the agreements was comparable to a rental term, obviously allowing the defendant to use the same copy of software in other transactions, and (e) the customer was not given the software manufacturer's registration card unless the full purchase price was paid.

c. **Software upgrades.** Judge Wexler also held the defendant liable for renting customers post-December 1, 1990 upgrades of programs it acquired before December 1, 1990. Judge Wexler held that the company's right to lawfully rent software acquired before December 1, 1990 did not extend to later upgrades of the same programs.

3. The opportunities for "sham" software transactions over the Internet are even greater than through traditional channels of retail trade. As more companies market their software over the Internet, the need to police the 'net for infringement will increase. This is particularly true because of the number of people who, for ideological reasons, believe that software should be freely available.

E. The Fair Use Defense

1. **What constitutes fair use?** Fair use is a complete defense to copyright infringement. 17 U.S.C. § 107. The defense applies where a work is used "for purposes such as criticism, comment, news reporting, teaching . . . scholarship or research . . . ." *Id.* In evaluating whether the fair use defense is available, courts must evaluate (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. *Id.*

2. **Reverse engineering of software.**

a. Disassembly of object code was held to be a fair use in *Sega Enterprises Ltd. v. Accolade, Inc.,* 977 F.2d 1510 (9th Cir. 1992) because (a) disassembly was necessary to analyze those aspects of the program which were unprotectable, and (b) Accolade had a legitimate interest in analyzing those aspects of the program (to determine how to make its cartridges compatible with the Genesis console); *see also Sony Computer Entertainment, Inc. v. Connectix Corp.,* 203 F.3d 596, 607 (9th Cir. 2000).

b. Disassembly was held not to be a fair use in *Atari Games Corp. v. Nintendo of America Inc.,* 975 F.2d 832, 834 (Fed. Cir. 1992) because Atari did not own an authorized copy of the plaintiff's program, which is a precondition for invoking the fair use defense. In dicta, the court wrote that intermediate copying is fair use when the nature of the work makes such copying necessary to understand the ideas and processes inherent in the program. Reverse engineering object code to discern the unprotectable ideas therefore may be fair use, the Federal Circuit wrote, provided that the reproduction is limited in scope and does not involve commercial exploitation of the protected aspects of the work.

c. For a more extensive discussion of reverse engineering as fair use, *see* William S. Coats & Heather D. Rafter, "The Games People Play: *Sega v. Accolade* and the Right to Reverse Engineer Software," 15 Hastings Communications & Entertainment L.J. 557 (1993).

3. **Parody.** *Campbell v. Acuff-Rose Music, Inc.,* 510 U.S. 569 (1994) (sampling of a copyrighted song may be fair use when used in a new parody work). Parody is not per se fair use. In order to constitute a fair use parody a work generally must be targeted at the original work and not merely borrow its style.

4. **Taping television transmissions for future viewing.** The practice of recording television broadcasts on videocassette recorders is a fair use when the copying is undertaken for private, non-commercial purposes. *Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417 (1984). The decision was supported by evidence that this form of copying represented "time shifting," or the practice by viewers of recording television transmissions to watch at more convenient times.

5. **Photocopying articles for convenience.** *American Geophysical Union v. Texaco, Inc.,* 37 F.3d 881 (2d Cir. 1994), pet. for cert. filed (Apr. 24, 1995); *American Geophysical Union v. Texaco, Inc.,* 60 F.3d 913 (2d Cir. 1995).

a. **1994 opinion.** The Second Circuit held that a scientist's practice of photocopying individual scientific articles that he kept in personal files in his office as a matter of convenience (to save the time it otherwise would have taken to retrieve the articles in journals maintained in Texaco's library) did not constitute fair use in view of the predominantly archival (rather than research-oriented) purpose of the copying, and because of the harm this practice caused to the publisher's market for licensing photocopying. The majority analyzed the scientist's copying as an "intermediate use," as that term was used in *Sega Enterprises Ltd. v. Accolade, Inc., supra,* because Texaco's photocopying "served, at most, to facilitate [the scientist's] research, which in turn might have led to the development of new products and technology that could have improved Texaco's commercial performance." 37 F.3d at 889. Unlike in

Sega Enterprises, the Second Circuit did not find the fair use defense applicable.

b. **Amended opinion.** The Second Circuit took the unusual step of amending its opinion in July 1995, *after* Texaco had asked the Circuit to defer ruling on its petition for rehearing *en banc* based on the parties' agreement in principle to settle the case. In his amended opinion, Judge Newman emphasized that the decision rested on a finding of "institutional, systematic copying." 60 F.3d at 931. He wrote that "[w]e do not deal with the question of copying by an individual for personal use in research or otherwise (not for resale), recognizing that under the fair use doctrine or the *de minimis* doctrine, such a practice by an individual might well not constitute an infringement." *Id.* at 916; D. Pines, "Aim to Narrow Circuit Ruling on 'Fair Use'; Amended Decision Issued in Controversial Case," N.Y.L.J., July 19, 1995, at 1. Although the Second Circuit purports to distinguish between individual and institutional copying, this distinction is not clearly apparent from the facts of the *Texaco* case itself, making further litigation likely.

c. **Law lags behind technology.** The *Texaco* opinion also provides an example of how changes in the law lag behind technological innovations. In *Texaco,* the Second Circuit lamented congressional inaction, writing that, "[a]s with the development of other easy and accessible means of mechanical reproduction of documents, the invention and widespread availability of photocopying technology threatens to disrupt the delicate balances established by the Copyright Act." 37 F.3d at 885-86.

d. **Implications online.** The problem of technology facilitating copyright infringement is even more acute online, where, for example, information (in the form of sound, video, images and/or written text) retrieved in digital form for a fee from an online database can be attached to an email message and transmitted in a matter of seconds to hundreds, or even thousands of people. While widespread dissemination of protected material would constitute infringement, the parameters of "fair use" in Cyberspace are unclear. For example, is it "fair use" for someone to attach an electronic version of an article downloaded via the Internet to a private email message sent confidentially to a friend, much in the way a person might clip an article from a newspaper and mail it to someone? Since many people, including lawyers, maintain files in electronic form, this question is not merely hypothetical. *See* Ian C. Ballon, "Determining Fair Use in Cyberspace," L.A. Daily Journal, Sept. 6, 1995, at 7.

6. **The retransmission over the Internet of infringing material (the Church of Scientology cases).** The extent to which protected material may be posted online for the purpose of criticism is being litigated at the present time in three lawsuits involving former members

of the Church of Scientology (and in a fourth suit involving a nonmember) who have posted confidential Scientology documents (that the church contends constitute trade secrets) online, ostensibly to embarrass and criticize the church and expose Scientology teachings. In all three suits against former Church members, the defendants include both the individuals who posted the protected works and their Internet access providers.

a. In *Religious Technology Center v. F.A.C.T.Net, Inc.,* 901 F. Supp. 1519 (D. Colo. 1995), Judge Kane denied plaintiff's motion for a preliminary injunction finding defendant's posting of unpublished Scientology documents a fair use "to advance understanding of issues concerning the Church which are the subject of ongoing public controversy," in part because there was no "potential for financial loss to the church."

b. **Netcom litigation - the individually named defendant.** In a much more thorough analysis, Judge Whyte of the Northern District of California rejected defendant Erlich's fair use defense in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 923 F. Supp. 1231 (N.D. Cal. 1995), finding the defense inapplicable because of the high percentage of plaintiffs' works copied, the extent of verbatim copying and the minimal amount of added criticism or commentary. Judge Whyte also ruled that the scope of permissible fair use was narrower in this case because plaintiff's works were unpublished. Otherwise, the informational (as opposed to creative) nature of the works would have allowed for a broader interpretation of fair use. 923 F. Supp. at 1246. Defendant Erlich's argument that a preliminary injunction would operate as a prior restraint on his First Amendment rights was rejected on the grounds that the fair use defense incorporated in the 1976 Copyright Act "embodies a balance between the rights of copyright holders, guaranteed by the Constitution, U.S. Const. art. I, § 8, and the protections of the First Amendment." 923 F. Supp. at 1258 (citations omitted).

c. **Netcom litigation - the internet access provider.** In a later opinion on November 21, 1995, Judge Whyte ruled that there was a genuine question of fact as to whether Netcom, the Internet access provider for the BBS where Erlich posted his infringing messages, had a valid fair use defense. The court denied Netcom's motion for summary judgment in light of evidence that it knew that Erlich's use was infringing and had the ability to prevent further distribution. In analyzing the first fair use factor, the purpose and character of the use, the court concluded that Netcom's "use" of plaintiffs' works was to carry out its commercial function as an Internet access provider, writing that "Netcom's use, though commercial, also benefits the public in allowing for the functioning of the Internet and the dissemination of other creative

works, a goal of the Copyright Act." 907 F. Supp. at 1379 (citations omitted). The court also noted that, although Netcom gained financially from its distribution of messages over the Internet, its financial incentive was unrelated to the infringing activity and Netcom received no direct financial benefit from Erlich's acts of infringement. The court determined that the second factor, the nature of the copyrighted work, was not important to its fair use analysis because "Netcom's use of the works was merely to facilitate their posting to the Usenet, which is an entirely different purpose than plaintiffs' use (or, for that matter, Erlich's use) . . . ." Id. at 1379 (citations omitted). In analyzing the third factor, the amount and substantiality of the portions used, the court deemed immaterial the extent of Netcom's copying (despite the fact that it was substantial) because Netcom made available to the Usenet exactly what was posted by Erlich; "Netcom copied no more of plaintiffs' works than necessary to function as a Usenet server. Like the defendant in *Sega v. Accolade,* Netcom had no practical alternative way to carry out its socially useful purpose; a Usenet server must copy all files, since the prescreening of postings for potential copyright infringement is not feasible." *Id.* at 1380, *citing Sega Enterprises, Ltd. v. Accolade, Inc.,* 977 F.2d 1510, 1526-27 (9th Cir. 1992). Finally, the court found that there was a genuine issue of fact with respect to the fourth factor, the effect of the use upon the potential market for the work, which the court deemed to be the most significant factor. 907 F. Supp. at 1380.

d. **Lerma - initial orders.** In *Religious Technology Center v. Lerma,* 897 F. Supp. 260 (E.D. Va. 1995), the court entered a temporary restraining order against Arnaldo Lerma, a former Scientology member, and Digital Gateway Systems, Lerma's Internet access provider. Thereafter, Lerma gave copies of the documents posted online to a Washington Post reporter who quoted small excerpts in a news article about the lawsuit. The reporter, Marc Fisher, and the Washington Post subsequently were added as defendants to the lawsuit. On August 30, 1995, the court denied plaintiff's motion for a temporary restraining order and preliminary injunction against Fisher and the Washington Post on fair use grounds in large measure because the Washington Post was able to acquire the same documents quoted in the news article by photocopying court records in another lawsuit pending in California, during a brief period of time when the court records in that case were not under seal. In a later opinion, on November 28, 1995, the court granted summary judgment in favor of Fisher and the Washington Post. *Religious Technology Center v. Lerma,* 908 F. Supp. 1362 (E.D. Va. 1995). However, Judge Brinkema ordered the Washington Post defendants to refrain from making additional copies of the documents or filing them with the court except under

seal. In focusing its fair use analysis on the small excerpts of plaintiff's works reproduced in the *Washington Post* article, the court apparently overlooked the issue of whether the Washington Post's wholesale photocopying of protected works from a court file constituted copyright infringement. *See American Geophysical Union v. Texaco, Inc.,* 60 F.3d 913 (2d Cir. 1995); *supra* § II(E)(5).

e. **Lerma - First Amendment arguments.** In still another ruling in *Religious Technology Center v. Lerma,* 908 F. Supp. 1353 (E.D. Va. 1995), the court on November 29, 1995 denied plaintiffs' motion for a preliminary injunction against defendants Lerma and Digital Gateway Systems and denied plaintiffs' "Emergency Motion for Reconsideration" of the court's August 30, 1995 order denying injunctive relief against the *Washington Post* defendants. In so ruling, Judge Brinkema rejected plaintiffs' argument that they were being denied their right to free exercise of their religion because, according to the Scientology religion, the texts at issue had to be kept confidential (except from a select few who had achieved certain spiritual levels). Plaintiffs had argued that dissemination of their confidential materials would decimate the scientology religion, and therefore was comparable to "compelling a Protestant to dispute the Resurrection, ordering a fundamentalist to read the Bible [non-literally], compelling an observant Jew to eat pork, or compelling an observant Catholic to have an abortion." Judge Brinkema, however, rejected these analogies, and wrote that, "[i]n their effort to enjoin the Post, the RTC is essentially urging that we permit their religious belief in the secrecy of the AT documents to 'trump' significant conflicting constitutional rights. In particular, they ask us to dismiss the equally valid First Amendment protections of freedom of the press." Stated differently, the court characterized plaintiffs' argument as a request to "allow the Free Exercise Clause to deflate the doctrine of fair use as embodied in the copyright statute . . . ." In the alternative, the court ruled that plaintiffs were barred from injunctive relief by the unclean hands doctrine because their zealous prosecution of this lawsuit and the related *F.A.C.T.Net* case were really intended to stifle legitimate criticism of the Church, rather than merely protect confidential works.

f. In *Religious Technology Center v. Ward*, Case No. 96-20207 (N.D. Cal. Mar. 21, 1996), the Church obtained a temporary restraining order against a nonmember who solicited Church documents in Internet postings and republished them online ostensibly to protect the First Amendment. D. Yaffe, "Scientologists Get TRO in Internet Copyright Battle," The Recorder, Mar. 25, 1996, at 4. The case has been assigned to Judge Whyte, who also is presiding over the *Netcom* litigation.

7. **Web browsing.** When a user browses through pages on the worldwide web (or elsewhere) screen displays are automatically downloaded to cache or screen memory. In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361 (N.D. Cal. 1995), Judge Whyte wrote in dicta that browsing could cause an infringing copy to be made in screen memory, but that such copying would be deemed to be fair use because "the temporary copying involved in browsing is only necessary because humans cannot otherwise perceive digital information." *Id.* at 1378 n.25. Judge Whyte characterized digital browsing as "the functional equivalent of reading, which does not implicate the copyright laws and may be done by anyone in a library without the permission of the copyright owner." *Id.; see* § II(F)(7)(e).

8. **Shareware.** In *Storm Impact, Inc. v. Software of the Month Club,* 13 F. Supp. 2d 782 (N.D. Ill. 1998), the court ruled that the defendant's practice of aggregating (free) shareware software from the Internet, which it sold as part of CD ROM compilations, constituted copyright infringement in violation of the terms of the plaintiff's shareware license. *Storm Impact* is a reminder that material may not necessarily be freely copied merely because it is accessible without charge online.

9. **Copying by visual search engines.** In *Kelly v. Arriba Software Corp.*, 77 F. Supp. 2d 1116 (C.D. Cal. 1999), a court ruled that the practice of a visual search engine - in making unauthorized thumbnail copies of photographs located on sites responsive to user search requests - constituted a fair use under copyright law. The court deemed it significant that the images were generated indiscriminately based on user requests and that they served a functional, rather than creative purpose (to facilitate searching and indexing practices). The court also considered it important that thumbnail images could not be enlarged into "useful images" and that the copies made had little or no negative impact on the market for plaintiff's genuine images.

F. The Third-Party Liability of Online Content and Access Providers

1. Direct Liability

a. **Strict liability.** Under the 1976 Copyright Act, liability for direct infringement may be imposed regardless of a defendant's intent. Although a party's innocence may color the way a case is decided, culpability technically is only relevant in determining the amount of an award of statutory damages (which may be reduced to as little as $200 in cases of innocent infringement; *see* 17 U.S.C. § 504(c)) or in limited circumstances where a work first published prior to March 1, 1989, did not contain a copyright notice. *See id.* § 405(b). As a practical matter, this means that a defendant's alleged innocence rarely will be a significant legal issue in a direct infringement case involving more recent works since a copyright plaintiff has sole discretion whether to

elect statutory damages in lieu of actual damages (and intent is not considered in assessing actual damages). *See id.* § 504(c). A defendant's bad faith, on the other hand, may be relevant in negating a defense of fair use. *See Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 923 F. Supp. 1231, 1244 (N.D. Cal. 1995).

b. **Volitional conduct required**. Some courts have held that even though the Copyright Act imposes strict liability, online providers may not be held directly liable merely because infringing content has been posted online. Thus, courts hold that some element of volitional conduct is required. *See Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) (Usenet postings; in order to find direct liability, "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."); *Sega Enterprises Ltd. v. MAPHIA, 9*48 F. Supp. 923, 932 (N.D. Cal. 1996) (no evidence that the BBS operator caused infringing copies to be made merely by operating a BBS where third parties posted infringing software); *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997) (company which hosted a website on which infringing material was posted held not liable for direct infringement because, even though it "provide[d] a service somewhat broader than the . . . . Internet access provider in Religious Technology Center . . . [it] only provided the means to copy, distribute or display plaintiff's works, much like the owner of a public copy machine used by a third party to copy protected material."); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.,* 982 F. Supp. 503 (N.D. Ohio 1997) ("some element of direct action" is required). *But see Playboy Enterprises, Inc. v. Frena,* 839 F. Supp. 1552 (M.D. Fla. 1993) (holding a BBS operator liable for infringing photographs potentially posted by a third party because the Copyright Act imposes strict liability).

2. **Culpable conduct required for contributory infringement.** A BBS systems operator or other online service provider may be held liable for contributory copyright infringement under certain circumstances*. See Sega Enterprises Ltd. v. MAPHIA,* 857 F. Supp. 679, 686 (N.D. Cal. 1994) ("'[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another,' may be held liable as a contributory infringer."); *see generally Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417, 435 (1984) ("The absence of . . . express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity for vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another").

3. **Vicarious liability.** More controversial is the question of whether an online service provider may be held vicariously liable for infringing acts that take place online without the service provider's knowledge or encouragement. Vicarious liability may be imposed where the defendant (1) has the right and ability to supervise the infringing activity, and (2) has a direct financial interest in such activities. *E.g., Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259 (9th Cir. 1996). By definition, vicarious liability, like direct liability, is imposed without regard to defendant's intent.

a. **NII White Paper.** The Clinton Administration's Information

Infrastructure Task Force, in the NII White Paper issued on September 5, 1995, has taken the position that online service providers may be held vicariously liable, citing the so-called "dance hall" cases where club owners were held liable for copyright infringement based on the unauthorized public performance of musical works by bands they hired, even though the owners had no knowledge of the infringement and had expressly warned the bands not to perform copyrighted works without a license. NII White Paper at 114 & n.355, *citing Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co.,* 36 F.2d 354 (7th Cir. 1929); *Shapiro, Bernstein & Co. v. H.L. Green Co.,* 316 F.2d 304, 307 (2d Cir. 1963); *Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Ass'n, Inc.,* 554 F.2d 1213 (1st Cir. 1977); and *KECA Music Inc. v. Dingus McGee's Co.,* 432 F. Supp. 72 (W.D. Mo. 1977). This position is controversial, however, and many people believe that online service providers are more akin to common carriers like phone companies than private dance hall operators.

b. **Canadian position**. In contrast to the U.S. government, the Canadian government panel analyzing Internet-related issues has expressly rejected the notion of vicarious liability for online service providers. See Final Report of the Information Highway Advisory Council (**http://www.emp.ca/opengov/nabst**). The Report states that, although BBS owners and operators are not common carriers, "a defense mechanism should be provided for those instances where it can be demonstrated that they did not have actual or constructive knowledge of the infringing or offensive material and where they have acted reasonably to limit potential abuses."

c. For further analysis, *see generally* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards A Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet,* 18 Hastings J. Communications & Ent. L. 729 (1996).

4. ***Playboy Enterprises, Inc. v. Frena,*** 839 F. Supp. 1552 (M.D. Fla. 1993).

a. **Facts:** Defendant George Frena operated a subscription computer bulletin board service (BBS). For a fee, subscribers could log onto Frena's BBS and upload and download digitized copies of photographs. Frena argued that he allowed subscribers to upload whatever they wanted onto the BBS. At least 170 images available in Frena's BBS were taken from 50 of Playboy's copyrighted magazines. Frena's name, BBS name and telephone number appeared on each of the infringing images.

b. **Holding:** The trial court granted partial summary judgment for the plaintiff, holding that Frena had violated Playboy's exclusive rights as a copyright owner to distribute and display its photographs. Id. at 1556-57. The court rejected Frena's argument that he was unaware of the infringement since intent or knowledge is only relevant to the issue of statutory damages, not liability for copyright infringement. *Id.* at 1559.

5. ***Sega Enterprises Ltd. v. MAPHIA***, 857 F. Supp. 679 (N.D. Cal. 1994).

a. **Facts:** Defendants operated a computer bulletin board called "MAPHIA" on which unauthorized copies of plaintiff's copyrighted videogames were uploaded and downloaded by bulletin board

subscribers. Defendants actively encouraged subscribers to upload and download bootlegged copies of Sega's videogames and even marketed hardware and software that could be used to make unauthorized copies of Sega videogames, which in genuine form are stored on a cartridge in a read-only memory (ROM) chip.

b. **Holding:** preliminary injunction granted. Defendants were held liable for copyright infringement as contributory infringers based on their "provision of facilities, direction, knowledge and encouragement . . . ." *Id.* at 686-87.

c. **Isolated acts of infringement.** In both *Frena* and *MAPHIA,* the plaintiffs introduced evidence of the defendant's complicity in acts of infringement. BBS operators generally should not be held contributorily liable for random acts of infringement which they have not encouraged (either actively or tacitly). *See Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417, 442 (1984) (liability for contributory infringement generally requires a showing that the good (or service) in question is not widely used for legitimate, unobjectionable purposes). Under the "staple article of commerce doctrine," courts "must strike a balance between a copyright holder's legitimate demand for effective - not merely symbolic - protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce." *Id.*

6. ***Frank Music Corp. v. CompuServe Inc.,*** No. 93 Civ. 8153 (S.D.N.Y 1993).

a. **Plaintiff's claims.** Music publishers filed a class action suit against CompuServe alleging that CompuServe Musical Bulletin Board allowed users to upload and download digitized versions of copyright songs. "Legal Beat: Coin Slot for CompuServe's Virtual Jukebox," Wired, July 1994.

b. **Settlement terms.** The case settled in 1995 with CompuServe agreeing to (a) pay a rights fee to the National Music Publishers Association (NMPA) for offering music online that could be downloaded and played by subscribers, and (b) help outside content providers electronically license rights to music from NMPA. Edupage, Nov. 9, 1995, *citing* The Wall Street Journal, Nov. 8, 1995, at B11.

7. ***Religious Technology Center v. Netcom On-Line Communication Services, Inc.,*** 907 F. Supp. 1361 (N.D. Cal. 1995).

a. **Procedural Background**: In February 1995, the Church of Scientology brought suit in federal court in San Jose against Dennis Erlich, a former Scientology minister who allegedly posted copyrighted material authored by L. Ron Hubbard on a Usenet group named "alt.religion.scientology"; Netcom On-Line Communication Services, an Internet access provider; and Tom Klemesrud, the operator of the BBS where Erlich posted his material (which was connected to the Internet via Netcom). Plaintiffs allege that Erlich stole their trade secrets, that Erlich's postings infringe plaintiffs' copyrights and that Netcom and Klemesrud are also liable for Erlich's alleged copyright infringement and misappropriation of trade secrets. A preliminary injunction issued against Erlich remains in effect. *See Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 923 F. Supp. 1231 (N.D. Cal. 1995); supra § II(E)(6)(b).

b. **November 1995 opinion:** On November 21, 1995, Judge Whyte denied Netcom's motion for summary judgment and Klemesrud's motion for judgment on the pleadings because he found a triable issue of fact on plaintiffs' claim for contributory infringement. Judge Whyte found no evidence to support claims of direct infringement against Netcom or Klemesrud or vicarious liability against Netcom, although he granted plaintiffs thirty days' leave to amend their complaint to state a claim for vicarious liability against defendant Klemesrud, if they could do so in good faith. Judge Whyte also denied plaintiffs' application for a preliminary injunction against Netcom and Klemesrud.

c. **Facts relevant to the motions:** After failing to convince defendant Erlich to stop posting scientology documents on the "alt.religion.scientology" Usenet group, plaintiffs contacted defendants Klemesrud and Netcom demanding that they take action to stop Erlich's postings. Klemesrud responded by asking for proof that plaintiff owned copyrights to the works posted by Erlich; plaintiffs refused Klemesrud's request as unreasonable. Netcom took no action after it was notified by plaintiffs, claiming that it could not block Erlich's postings without shutting out all of the users of Klemesrud's BBS. Unlike on-line services that provide content, such as CompuServe, America Online, or Prodigy, Netcom, as merely an Internet access provider, does not create or control the content of the information available to its subscribers.

The parties did not dispute the basic processes that occurred when Erlich posted his allegedly infringing messages to the "alt.religion.scientology" newsgroup:

> Erlich connects to Klemesrud's BBS using a telephone and a modem. Erlich then transmits his messages to Klemesrud's computer, where they are automatically briefly stored. According to a prearranged pattern established by Netcom's software, Erlich's initial act of posting a message to the Usenet results in the automatic copying of Erlich's message from Klemesrud's computer onto Netcom's computer and on to other computers on the Usenet. In order to ease transmission and for the convenience of Usenet users, Usenet servers maintain postings from newsgroups for a short period of time - eleven days for Netcom's system and three days for Klemesrud's system. Once on Netcom's computers, messages are available to Netcom's customers and Usenet neighbors, who may then download the messages to their own computers. Netcom's local server makes available its postings to a group of Usenet servers, which do the same for other servers until all Usenet sites worldwide have obtained access to the postings, which takes a matter of hours.

907 F. Supp. at 1367-68.

d. **Erlich's transmissions held to create "copies" on Klemesrud's BBS and Netcom's computers.** The court, applying *MAI Systems Corp. v. Peak Computer, Inc.,* 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994) (supra § II(A)(2)(b)(1)), held that

Erlich's act of sending a message to the "alt.religion.scientology" Usenet group caused "copies" of plaintiffs' works to be created on both Klemesrud's and Netcom's storage devices (even though the messages remained on their systems for at most 11 days).

e. **Netcom not liable for direct infringement.** The court held that Netcom could not be held liable for direct infringement, even though the Copyright Act is a strict liability statute, because "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party." 907 F. Supp. at 1370.

> (1) ***MAI* Distinguished.** Judge Whyte wrote that "Netcom's actions, to the extent that they created a copy of plaintiffs' works, were necessary to having a working system for transmitting Usenet postings to and from the Internet. Unlike the defendant in MAI, neither Netcom nor Klemesrud initiated the copying. . . . Netcom's and Klemesrud's systems can operate without any human intervention. Thus, unlike *MAI,* the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean Netcom has caused the copying." *Id.* at 1368-69.
>
> (2) **Ruling Contradicts NII White Paper.** Disagreeing with the recommendations of the NII White Paper that BBS operators be held strictly liable, Judge Whyte concluded that "[t]he court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits. Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement." *Id.* at 1372-73.

f. **Netcom's potential liability for contributory infringement**. The court held that a triable issue of fact existed as to whether Netcom could be held liable for contributory infringement, which the court wrote is imposed "where the defendant, 'with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.'" 907 F. Supp. at 1373, *quoting Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971). The court found that it was undisputed that Netcom initially did not know that Erlich was infringing, but there was a question of fact about whether Netcom knew or should have known that Erlich had infringed plaintiffs' copyrights after it received notice from plaintiffs and failed to investigate. Although a mere unsupported allegation of infringement may not automatically put a defendant on notice of infringing activity,

> where works contain copyright notices within them, as here, it is difficult to argue that a defendant did not know

> that the works were copyrighted. To require proof of valid registrations would be impractical and would perhaps take too long to verify . . . the court is more persuaded by the argument that it is beyond the ability of a BBS operator to quickly and fairly determine when a use is not infringement where there is at least a colorable claim of fair use. Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is a likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.

Id. at 1374.

g. **Netcom not liable for vicarious infringement.** The court held that plaintiffs failed to show a triable issue of fact on the issue of whether Netcom received a direct financial benefit from Erlich's infringement, precluding plaintiffs' claim for vicarious liability. The court wrote that to prove vicarious liability, a plaintiff must show the defendant (1) had the right and ability to control the infringer's acts and (2) received a direct financial benefit from the infringement. 907 F. Supp. at 1375, c*iting Shapiro, Bernstein & Co. v. H.L. Green Co.,* 316 F.2d 304, 306 (2d Cir. 1963). The court also reiterated that unlike contributory infringement, knowledge need not be shown.

> (1) **Right and ability to control.** The court found conflicting evidence on the issue of whether Netcom had the ability to control Erlich's infringing conduct. As merely an access provider, Netcom does not create or control the content of the information available to its subscribers, and it does not monitor messages as they are posted. Netcom claimed that it could not limit Erlich's access to the Usenet without "kicking off all 500 subscribers of Klemesrud's BBS." However, Netcom had, in the past, suspended the accounts of subscribers who have violated its terms and conditions (for example, when individuals had commercial software in their posted files). In addition, Netcom admitted during the litigation that (while not currently configured to do so) it might have been possible to reprogram its system to screen postings containing particular words or coming from particular individuals. 907 F. Supp. at 1375-76.
>
> (2) **Direct financial benefit.** The court found that plaintiffs were unable to show that Netcom received a direct financial benefit from the infringing activities of its users. Netcom receives a fixed fee and no evidence was presented that the infringement by Erlich, or any other user of Netcom's services, in any way enhanced the value of Netcom's services to subscribers or attracted new subscribers. 907 F. Supp. at 1377. *But see Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259 (9th Cir. 1996) (holding that a plaintiff adequately stated a

claim for vicarious liability against the operator of a flea market by alleging that defendants benefited financially from fixed daily rental fees paid by each infringing vendor, and rejecting defendant's argument that the financial benefit prong of the test for vicarious liability could only be satisfied if the defendant earned a commission directly tied to the sale of particular infringing item).

h. **Netcom's First Amendment argument.**

(1) **Chilling effect on Internet access providers**. Netcom argued that plaintiffs' theory of liability would chill the use of the Internet and therefore contravene the First Amendment. Judge Whyte agreed in dicta that there could be a serious chilling effect if Usenet servers were responsible for all messages coming through their systems, but he wrote that he was "not convinced that Usenet servers are directly liable for causing a copy to be made, and absent evidence of knowledge and participation or control and direct profit, they will not be contributorily or vicariously liable." He further wrote that "[t]he copyright concepts of the idea/expression dichotomy and the fair use defense balance the important First Amendment rights with the constitutional authority for 'promot[ing] the progress of science and the useful arts . . . .'" 907 F. Supp. at 1377.

(2) **User liability: browsing as copyright infringement.** Netcom also argued that plaintiffs' theory of liability would have a chilling effect on users, who could be found liable for copyright infringement merely by browsing infringing works. Judge Whyte wrote in dicta that browsing "technically causes an infringing copy of the digital information to be made in the screen memory" since under *MAI Systems Corp. v. Peak Computer, Inc.,* 911 F.2d 511 (9th Cir. 1993) (*supra* § II(A)(2)(b)(1)), *cert. dismissed,* 510 U.S. 1033 (1994), a copy is fixed when information is temporarily placed in RAM, including in the case of browsing, screen RAM. Judge Whyte noted, however, that it was highly unlikely, as a practical matter, that a copyright owner could prove infringement by browsing, or would want to sue an individual browser. Judge Whyte also wrote that absent a commercial or profit-depriving use, digital browsing would be deemed a fair use. *See supra* § II(E)(7).

i. **Netcom's fair use defense.** The court found a material factual dispute on Netcom's entitlement to the fair use defense in light of evidence that, after it received notice, it knew that Erlich's use was infringing and had the ability to prevent its further distribution. *See supra* § II(E)(6)(c).

8. **Netcom Settlement.** In August 1996, the Church of Scientology reached agreement with Netcom to settle its copyright infringement action. As part of the settlement, Netcom announced new guidelines entitled "Intellectual Property Rights on the Internet," which are now distributed to all Netcom subscribers. The statement

provides that computers whose host name or address includes "Netcom.com" are required to abide by Netcom's terms and conditions ("Terms"). The Terms include the prohibition on "using Netcom services to unlawfully distribute the intellectual property of others, regardless of format of property." The procedures for addressing postings challenged as improper are as follows:

> 1. The complainant shall provide Netcom and the posting party with notice of the alleged violation with enough specific detail to allow Netcom to locate the posting. The complainant shall ask the posting party to remove the material, pending Netcom's investigation.
>
> 2. Complainant shall substantiate its claim by providing Netcom with:
>
> > a. The copyright or trademark registration number;
> >
> > b. A copy of the underlying work; and
> >
> > c. A good faith certification, signed under penalty of perjury, the original work is the property of complainant, that a significant portion of that work has been copied, and that the use of the work is not defensible.
>
> 3. Upon receipt of notice from the complaining party, the posting party may provide Netcom with a response to the complaint.
>
> 4. While Netcom is investigating the complaint, Netcom will temporarily remove or deny access to the challenged material, to protect the rights of all involved.
>
> 5. If Netcom concludes that complainant has raised a legitimate claim, it will continue to deny access to the challenged material. If Netcom concludes that complainant has not raised a legitimate claim, Netcom will restore access to the challenged material.

9. ***Sega Enterprises Ltd. v. MAPHIA,*** 948 F. Supp. 923 (N.D. Cal. 1996). In a subsequent opinion in *Sega Enterprises, Ltd v. MAPHIA, J*udge Claudia Wilken adopted - and extended in part - Judge Whyte's analysis of third party liability. For a discussion of the facts, *see supra* § II(F)(5).

> a. **Direct liability.** Judge Wilken adopted Judge Whyte's analysis of direct liability, even though she acknowledged that the defendant's actions in *MAPHIA* were more participatory than in *Netcom.* Judge Wilken wrote that:
>
> > Sega has not shown that Sherman himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sherman operated his BBS, that he knew infringing activity was occurring, and that he solicited others to upload the games. However, whether Sherman knew his BBS users were infringing on Sega's copyright, or encouraged them to do so, has no bearing on whether Sherman directly caused the copying to occur . . . Sherman's actions as a BBS operator and copier seller are more appropriately analyzed under contributory or vicarious liability theories. . . . [B]ecause Sega has not shown that Sherman directly caused the copying, Sherman cannot be liable for direct infringement.

948 F. Supp. at 932 (citation and footnote omitted).

b. **Contributory liability.** Judge Wilken, in granting summary judgment in favor of Sega, reiterated her earlier ruling, on motion for preliminary injunction, finding the defendant liable for contributory infringement. *Id*. at 933. Judge Wilken did not reach the issue of vicarious liability.

10. ***Sega Enterprises Ltd. v. Sabella,*** Case No. C 93-04260 CW, 1996 U.S. Dist. LEXIS 20470 (N.D. Cal. Dec. 18, 1996). In a companion case to *Sega Enterprises Ltd. v. MAPHIA,* Sega obtained partial summary judgment in an infringement action brought against Sharon Sabella, the systems operator of a BBS called "The Sewer Line," where she was known by the pseudonym "Dirty Scum." Sabella was aware that her BBS contained a directory called "Genesis," which was a term she knew to be associated with videogames. File descriptors in this directory included the names of approximately 20 Sega games as well as the word "SEGA," which is a trademark owned by Sega. A number of Sega games, including prerelease versions, were posted on the BBS. Sabella also operated a separate business, Sharon's Data Systems, that sold Multi-Game Hunter Copiers, which could be used to copy games from Sega game cartridges to computer disks. Sharon's Data Systems advertised its products on The Sewer Line. Unlike the MAPHIA defendants, however, Sabella claimed not to have known that copyrighted videogames had been uploaded to her BBS. Judge Wilken nonetheless held her liable for contributory infringement, finding that she had reason to know of her subscribers' infringing activity.

11. ***Playboy Enterprises, Inc. v. Webbworld, Inc.***, 991 F. Supp. 543 (N.D. Tex. 1997), *aff'd mem.,* 168 F.3d 486 (5th Cir. 1999).

a. **Facts.** Defendants owned or operated a website that offered subscribers, for a flat $11.95 monthly fee, access to sexually-oriented photographs and images, which they obtained from Usenet postings. Although none of the defendants themselves posted any images owned by plaintiff, one of the defendants had developed a software program which automatically searched news feeds which defendants received from pre-determined adult newsgroups, discarded most of the text, and retained sexually-oriented images. Images were then transformed into "thumbnail" copies, which allowed multiple photographs to be displayed on a single page and facilitated faster downloading (subscribers could then select larger versions of the thumb-nail prints, if they so desired). The images were then automatically transferred to defendants' website for subscriber viewing. Webbworld normally stored and displayed about 40,000 to 70,000 images at a given time, with approximately 5,000 to 10,000 images added (and an equal number deleted) daily. Images remained online for an average of six days. During the time WebbWorld was in operation, hundreds of plaintiff's copyrighted images appeared on the website.

b. **Initial ruling.** In an earlier ruling, Judge Dale Saffels, sitting by designation, entered summary judgement in favor of plaintiff on the issue of direct liability on all but 16 of the allegedly infringing images found on defendant's site (which defendants argued had been tampered with after downloading from their site). Judge Saffels also held defendants Bentley Ives and Benjamin Ellis vicariously liable. 968 F. Supp. 1171, 1175 (N.D. Tex. 1997).

c. **Trial decision - direct liability.** In a more detailed ruling following trial on the disputed works, Judge Barefoot Sanders rejected defendants' argument that any infringing images on their site would have existed on the Usenet, whether or not Webbworld had provided access to the images to its subscribers. The court also rejected defendants' attempt to compare themselves to a mere conduit of information such as *Netcom in Religious Technology Center v. Netcom On-Line Communication Services, Inc.* 907 F. Supp. 1361, 1372-73 (N.D. Cal. 1995). In the words of the court, "Webbworld did not sell access; it sold adult images." Unlike in *Netcom,* Judge Sanders wrote that "Webbworld functioned primarily as a store . . . ," rather than "as a passive conduit of unaltered information." He wrote:

> Just as a merchant might re-package and sell merchandise from a wholesaler, so did Webbworld re-package (by deleting text and creating thumbnails) and sell images it obtained from various newsgroups. In contrast to the defendants in RTC, Webbworld took 'affirmative steps to cause the copies to be made'. . . . Such steps included using the ScanNews software to troll the Usenet for Webbworld's product.

d. **Trial decision - vicarious liability.** Judge Sanders, like Judge Saffels, found defendants Ives and Ellis vicariously liable. In rejecting the argument that defendants did not exercise control over the images automatically gathered and stored on its servers, the court wrote that "Webbworld exercised total dominion over the content of its site and the product it offered its clientele." The court in particular found significant the fact that defendants selected the newsgroups from which the images were automatically culled. For example, Judge Sanders noted that "a newsgroup named, for example, 'alt.sex.playboy' or 'alt.mag.playboy' might instantly be perceived as problematic from the standpoint of federal copyright law." The court further cautioned that:

> Webbworld might simply have refrained from conducting business until it had developed software or a manual system of oversight to prevent, or at least to minimize the possibility of, copyright infringement. . . . [H]aving developed and launched the ScanNews software for commercial use, Webbworld cannot now evade liability by claiming helplessness in the face of its "automatic" operation.

e. **Vicarious of liability investors**. The court declined to impose vicarious liability on a third defendant, James Gurkin, who contributed start-up capital to Webbworld and earned 25% of its net income. Although Gurkin derived financial benefit from the website the court found that he did not have the requisite supervisory authority over the infringing activity to justify the imposition of vicarious liability. Gurkin spent 3-5 hours per day responding to customer emails, but had no access to the ScanNews software, had no decision-making authority and did not become a shareholder until late in the company's existence.

G. Liability Limitations Under the Digital Millennium Copyright Act

1. **Copyright Liability Limitations.** The Online Copyright Infringement Liability Limitation Act incorporated as Title II of the Digital Millennium Copyright Act immunizes "Service Providers" (which as broadly defined under the Act would include ISPs, OSPs, search engines, portals and even owners of corporate intranets) from third party liability for damages, costs or attorney's fees under the Copyright Act, but only if an entity complies with a series of technical requirements. A Service Provider that satisfies three threshold prerequisites set forth in 17 U.S.C. § 512(I) (discussed below) may be entitled to immunity from copyright infringement liability for (1) transmitting, routing, and providing connections to infringing material (or what the statute refers to as "transitory digital network communications"); (2) system caching; (3) information stored by a user (the "user storage" limitation); or (4) linking or referring users to infringing material (the "information location tools" limitation).

2. **Exemption from Liability (under any theory of law) for Removing or Disabling Access to Content.** A Service Provider that otherwise has met the threshold requirements set forth in section 512(I) may be entitled to a broad exemption from liability under any theory of recovery for any good faith act to disable access to or remove material believed to be infringing, regardless of whether the material or activity is ultimately determined to be infringing.

There is one exception to the broad exemption provided for removing or blocking access to content. If a Service Provider receives a notification about allegedly infringing material stored at the direction of a subscriber, it must comply with the specific requirements of subparts (c)(3) and (g)(2) governing notification and counter notification in order to avoid all potential liability. Specifically, a Service Provider would have to satisfy the requirements of subpart (c)(3) to limit its potential liability to the copyright owner for infringement and comply with subpart (g)(2) to avoid any liability to its subscriber for disabling access to or removing content in response to a notification.

3. **Threshold Requirements.** In order to benefit from any of the new liability limitations created by the Act, a Service Provider must adopt and implement a policy of terminating the accounts or subscriptions of repeat infringers; inform subscribers and account holders of this policy; and accommodate and not interfere with "standard technical measures." To benefit from the user storage, caching and information location tools limitations, Service Providers also will need to designate agents to receive notification of alleged acts of infringement and comply with specific rules for removing or blocking access to content alleged to be infringing. For information on agent designation, *see* Designation of Agent to Receive Notification of Claims Infringement, 63 Fed. Reg. 59233 (Nov. 3, 1998). Further, to avoid liability to subscribers in cases where content is removed in response to a notification, Service Providers must comply with procedures governing counter notifications and potentially replace or restore access to content removed in response to a notification.

4. **Procedures for Notification and Counter Notification.** Where a Service Provider seeks to benefit from all liability limitations and the one exemption created by the Act, its agent must be prepared to act swiftly in response to Notifications and Counter Notifications. When a Notification that substantially complies with the requirements of the statute is received, a Service Provider must expeditiously remove or block access to the allegedly infringing content. Where the content was posted by a subscriber, the Service Provider must promptly notify its subscriber that it has removed or disabled access to the material. If the subscriber serves a Counter Notification on the agent, the Service Provider must promptly provide the original complainant with a copy of the Counter Notification. The Service Provider must then replace or restore access to the disputed content between the 11th and 14th

business day after the date on which it received the Counter Notification unless, within the first 10 business days, it receives a notice from the original complainant that it has filed suit to restrain the subscriber from engaging in infringing activity (in which case the Service Provider must take no further action pending a ruling by the court). Service Providers and other affected parties may recover damages if material misrepresentations are made in either Notifications or Counter Notifications.

5. **Benefits for Service Providers.** Service Providers that choose to comply with the Act - which went into effect on the day it was signed into law on October 28, 1998 - may limit their liability for acts of third party copyright infringement (although not the acts of their employees, unless the Service Provider is also a Nonprofit Educational Institution as defined under the Act) and may avoid liability for removing or disabling access to content believed in good faith to be infringing. Compliance may be time consuming, burdensome and costly for some companies, however, especially where Service Providers seek to benefit from the exemption for removing content (which requires them to meet tight time restrictions for forwarding Notifications to subscribers and responding to Counter Notifications).

6. **Benefits for Copyright Owners.** Copyright owners may be able to obtain the extra-judicial remedy of having infringing content removed from the Internet at a fraction of the cost of litigation if they understand the Act and know how to benefit from it. They also may be able to obtain the quick and inexpensive identification of the identity of alleged infringers who act pseudonymously. Copyright owners must understand and be prepared to respond within the tight time constraints imposed by the Act and how to properly draft substantially complying Notifications. Otherwise, copyright owners may needlessly incur substantial litigation fees to obtain relief that could be obtained from Service Providers who choose to comply with the Act virtually free of charge.

7. **More Information**. For more information on the Digital Millennium Copyright Act, see Ian C. Ballon & Keith M. Kupferschmid, "Third Party Liability under the Digital Millennium Copyright Act: New Liability Limitations and More Litigation for ISPs," The Cyberspace Lawyer, Oct. 1998, at 3 (**http://www.finnegan.com/finnegan/finnegan/library/millennium_cright_act.htm**).

H. Electronic Republication of Articles

1. In *Tasini v. New York Times Co.,* 206 F.3d 161 (2d Cir. 1999), the Second Circuit ruled that when *The New York Times* and certain other newspapers are digitized and placed in databases, they constitute new works (rather than permissible revisions under 17 U.S.C. § 201 (c)). Hence, the court ruled that permission must be obtained from any freelance authors who had not previously granted such rights.

2. Today it is common for publishing contracts to expressly define the parties' respective electronic publishing rights.

I. Criminal Copyright Infringement

1. *United States v. LaMacchia,* 871 F. Supp. 535 (D. Mass. 1994).

a. **Facts:** David LaMacchia, an MIT student, set up an electronic bulletin board with an Internet address (via MIT's computer network), through which he allegedly encouraged correspondents to upload popular software applications (including WordPerfect 6.0 and Excel 5.0) and computer games, which he transferred to a second encrypted

address where they could be downloaded by other users. LaMacchia was indicted for wire fraud. He successfully argued that his wire fraud conviction should be dismissed because he should have been charged with criminal copyright infringement.

b. **Criminal copyright liability must be predicated on commercial exploitation.** Unlike civil copyright law, a complaint for criminal copyright infringement requires a showing that the defendant's acts of infringement were pursued for purposes of commercial exploitation.

c. **The wire fraud statute was not applicable.** The court held that the wire fraud statute could not be stretched to fill apparent gaps in the Copyright Act. *But see United States v. Wang,* 898 F. Supp. 758 (D. Colo. 1995).

d. **Civil liability**. Assuming the same fact pattern, a defendant could be held civilly liable for contributory copyright infringement.

2. **NET Act.** Congress in 1997 enacted the No Electronic Theft (NET) Act, which is intended to reverse the practical consequences of *United States v. LaMacchia* by clarifying that electronic piracy of copyrighted works may be prosecuted under the wire fraud statute and amending the law so that criminal sanctions for copyright infringement may be imposed even where the defendant does not realize a commercial advantage or private financial gain. Criminal copyright infringement may be found if more than $1,000 worth of copies are made in any 180-day period).

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

III. TRADEMARK AND TRADE DRESS PROTECTION IN CYBERSPACE

A. Traditional Trademark Infringement on the Internet

1. **Elements of an infringement claim.**

a. To prevail on a claim for trademark infringement, a plaintiff must show (1) a protectable mark; and (2) likelihood of confusion as to the origin, affiliation or sponsorship of the defendant's product. *See, e.g., Goto.com, Inc. v. The Walt Disney Co.,* 202 F.3d 1199 (9th Cir. 2000) (logo infringement on a website).

b. To be protectable, a mark must be inherently distinctive or have acquired secondary meaning. *E.g., A.J. Canfield Co. v. Honickman,* 808 F.2d 291, 296-97 (3d Cir. 1986).

(1) A mark is "inherently distinctive" if it is fanciful, arbitrary or suggestive. *Two Pesos, Inc. v. Taco Cabana, Inc.,* 505 U.S. 763 (1992).

(2) A descriptive term, in contrast to one that is inherently distinctive, is entitled to trademark protection only if it has acquired secondary meaning. *E.g., A.J. Canfield Co. v. Honickman*, 808 F.2d 291, 296-97 (3d Cir. 1986). To prove secondary meaning, a plaintiff must show an association between an alleged mark and the product in the minds of relevant consumers. *E.g., Nutri/System, Inc. v. Con-Stan Indus.,* 809 F.2d 601, 605 (9th Cir. 1987)

(3) Generic terms are never protectable. *A.J. Canfield Co. v. Honickman, supra,* 808 F.2d at 296-97.

c. Likelihood of confusion is determined by a balancing test. The following factors are relevant: (1) strength of the mark; (2) proximity of the goods; (3) similarity of the marks; (4) evidence of actual confusion; (5) marketing channels used; (6) type of goods and the degree of care likely to be exercised by the purchaser; (7) defendant's intent in selecting the mark; and (8) likelihood of expansion of the product lines. *E.g., AMF Inc. v. Sleekcraft Boats,* 599 F.2d 341, 348-49 (9th Cir. 1979).

2. ***Playboy Enterprises, Inc. v. Frena,*** 839 F. Supp. 1552 (M.D. Fla. 1993).

a. **Facts:** *See supra* § II(F)(4)(a). Frena operated a BBS on which

subscribers uploaded and downloaded digitized copies of photographs from Playboy magazine. The original text was removed from the photographs and defendant's name, BBS name and telephone number was placed on each photograph. In addition, the trademarks "PLAYBOY" and "PLAYMATE" were used in file descriptions for 170 of the images. Defendant argued that the subscribers who uploaded the images provided the file descriptions. He also argued that he was unaware of the infringements and had allowed subscribers to upload anything they wanted on the BBS.

b. **Trademark infringement - file descriptors.** The court granted partial summary judgment for plaintiff, noting that bad faith need not be shown to establish trademark infringement under 15 U.S.C. § 1141(a). 839 F. Supp. at 1560-61.

c. **Unfair competition.** The court granted partial summary judgment for plaintiff on its unfair competition claim, finding that Frena's deletion of plaintiff's text from the photographs, addition of his own text to some of the images and appropriation of Playboy's photographs without attribution constituted acts of unfair competition under 15 U.S.C. § 1125(c). By falsely inferring and describing the origin of the photographs, Frena made it appear that Playboy Enterprises, Inc. authorized Frena's product. 839 F. Supp. at 1562.

d. **Reverse "passing off."** The court also held that Frena's removal of Playboy's trademarks from the photographs constituted "reverse passing off." *Id.*

e. **Comparison to Ninth Circuit rule on reverse "passing off."** Courts in the Ninth Circuit and the Southern District of New York have held that a "reverse palming off" claim may not be maintained where an adequate remedy is available under the Copyright Act. *E.g., Shaw v. Lindheim,* 919 F.2d 1353, 1364-65 (9th Cir. 1990); *Merchant v. Lymon,* 828 F. Supp. 1048, 1060 (S.D.N.Y. 1993); *see also Summit Machine Tool Manufacturing Corp. v. Victor CNC Systems, Inc.,* 7 F.3d 1434, 1438 (9th Cir. 1993) (holding that a claim for "reverse palming off" is unavailable "within the spheres protected by, or unintentionally left unprotected by, copyright and patent law.").

3. ***Sega Enterprises Ltd. v. MAPHIA,*** 857 F. Supp. 679 (N.D. Cal. 1994).

a. **Facts:** *See supra* § II(F)(5)(a). Plaintiff's "Sega" trademark appeared on the screen whenever a game that had been downloaded from the MAPHIA bulletin board was subsequently played. Some of the bootlegged programs posted on the bulletin board did not function as smoothly as genuine, commercially available Sega games, either because they were pre-release versions of games not yet commercially available, or because glitches had been introduced in the copying process. Id. at 684. The court concluded that bulletin board users and/or parties who may receive copies from the bulletin board "are likely to confuse the unauthorized copies downloaded and transferred from the MAPHIA bulletin board with genuine Sega videogame programs." *Id.*

b. **Holding:** preliminary injunction granted in part based on a finding of trademark infringement. The court reasoned that "confusion, if not on the part of bulletin board users, is inevitable on the part of third parties

who may see the copied games after they enter the stream of commerce." *Id.* at 688. In a subsequent opinion granting summary judgment in favor of Sega, the court emphasized that, as in *Playboy Enterprises, Inc. v. Frena,* the defendant "adopted the use of the Sega name as file descriptors on his BBS and the SEGA logo within those games, because he knew about the [infringing] use, and tacitly authorized it. Additionally, [defendant] used the mark when he created the file area that used the name Sega to identify the area where the game files would be located." 948 F. Supp. 938 (N.D. Cal. 1996).

c. **False designation of origin:** The court also found Sega likely to prevail on its unfair competition claim under the Lanham Act based on its finding that the public is likely to be deceived or confused by the similarity of marks shown on both the genuine product and the bootlegged programs uploaded to MAPHIA. 857 F. Supp. at 688.

4. S***ega Enterprises Ltd. v. Sabella***, Case No. C 93-04260 CW, 1996 U.S. Dist. LEXIS 20470 (N.D. Cal. Dec. 18, 1996).

a. **Facts:** *See supra* § II(F)(10). Sabella submitted a declaration in opposition to Sega's motion for summary judgment in which she stated that she did not know that Sega games were being uploaded and downloaded on her BBS and never used the mark herself in any of her BBS operations. Sega argued that Sabella's declaration was a sham and that she had reason to know that the Sega mark was being used as a file descriptor on her BBS and that the mark was displayed when those files were played.

b. **Trademark infringement:** The court held that a triable issue of fact existed on the issue of whether Sabella was liable for direct trademark infringement because Sega was unable to show unrefuted evidence that Sabella authored subscriber rules posted on her BBS which solicited others to upload "playable" files, or that she otherwise used the mark herself or knew that others were using it on her BBS.

c. **False designation of origin:** he court denied Sega's motion on its claim for false designation of origin because Judge Wilken found a triable issue of fact on the question of whether Sabella used or adopted the mark.

d. **State law claims:** Judge Wilken denied Sega's motion with respect to its California unfair competition claim, but granted the motion, and entered an injunction, pursuant to Cal. Bus. & Prof. Code §§ 1401 *et seq.,* which proscribes trade name infringement. The California statute authorizes a court to enjoin "any use" of a trade name that infringes on trade name rights recognized under California law, regardless of the enjoined party's specific knowledge or conduct.

5. **Contributory trademark infringement.**

a. Contributory trademark infringement may be found if a defendant (1) intentionally induces another to infringe a trademark, or (2) continues to supply a product knowing that the recipient is using the product to engage in trademark infringement. *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.,* 456 U.S. 844, 854-55 (1982); *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259 (9th Cir. 1996); Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards A Coherent Theory for*

Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet, 18 Hastings J. Communications & Ent. L. 729, 750-53, 761-64 (1996).

b. **No liability for offering an Internet-related service**. In *Lockheed Martin Corp. v. NSI,* 194 F.3d 980 (9th Cir. 1999), the Ninth Circuit ruled that a domain name registrar could not be held contributorily liable for registering infringing domain names after receiving two cease and desist letters because a registrar supplies a service - not a product - to third parties.

c. **Actual knowledge.** Two lower courts have ruled that a domain name registrar cannot be deemed to have received actual or constructive notice of an infringement merely because it was sent a cease and desist letter because of the inherent uncertainty in defining the scope of an owner's rights in a mark (which typically expand or contract over time). *See Lockheed Martin Corp. v. NSI*, 985 F. Supp. 949 (C.D. Cal. 1997), *aff'd on other grounds,* 194 F.3d 980 (9th Cir. 1999); *Academy of Motion Picture Arts and Sciences v. NSI,* 989 F. Supp. 1276 (C.D. Cal. 1997).

B. Dilution in Cyberspace

In January 1996, Congress passed the Federal Trademark Dilution Act, which is intended to protect famous marks, and does not require a showing of likelihood of confusion (or even that the plaintiff and defendant are competitors of one another).

1. **Elements of a claim.** The owner of a famous mark shall be entitled, "subject to the principles of equity and on such terms as the court deems reasonable," to an injunction against another person's commercial use of a mark or trade name, if such use begins after the plaintiff's mark has become famous and causes dilution of the distinctive quality of the mark. 15 U.S.C. § 1125(c)(1).

a. **Is a mark distinctive and famous?** In determining whether a mark is "distinctive and famous," a court "may consider factors such as, but not limited to" - (A) the degree of inherent or acquired distinctiveness of the mark; (B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used; (C) the duration and extent of advertising and publicity of the mark; (D) the geographical extent of the trading area in which the mark is used; (E) the channels of trade for the goods or services with which the mark is used; (F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought; (G) the nature and extent of use of the same or similar marks by third parties; and (H) whether the mark was registered on the principal register or under the 1881 or 1905 Trademark Acts. 15 U.S.C. § 1125(c)(1).

b. **Split in the circuits.** The Fourth Circuit has ruled that a plaintiff must show actual dilution, rather than likelihood of dilution, in order to obtain relief. *See Ringling Bros. - Barnum & Bailey Combined Shows, Inc. v. Utah Division of Travel Development,* 170 F.3d 449, 464 (4th Cir.), *cert. denied,* 120 S. Ct. 286 (1999). *But see Nabisco, Inc. v. PF Brands, Inc.,* 191 F.3d 208, 217, 223-25 (2d Cir. 1999) (rejecting this analysis).

c. **Niche market fame.** A mark may be considered famous and

distinctive within a narrow market if it is the same one in which a defendant operates. *See Syndicate Sales, Inc. v. Hampshire Paper Corp.,* 192 F.3d 633, 640-41 (7th Cir. 1999) (summarizing and harmonizing divergent lower court decisions).

d. **Dilution defined.** Dilution is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of - (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion or mistake or to deceive." 15 U.S.C. § 1127.

2. **Defenses.** The following are complete defenses to a dilution claim (15 U.S.C. §§ 1125(c)(3) and 1125(c)(4)):

a. Defendant's ownership of a valid registration under the 1881 or 1905 Trademark Acts or on the principal register;

b. Fair use of a famous mark in a comparative commercial advertisement or promotion to identify competing goods or services;

c. Noncommercial use of the mark; and

d. All forms of news reporting and news commentary.

3. **Relief.** The Act affords the owner of a famous mark the right to obtain injunctive relief and, in cases where the defendant willfully intended to trade on the owner's reputation or to cause dilution of the mark, damages, attorneys' fees and destruction of goods bearing the offending mark. 15 U.S.C. § 1125(c)(2).

4. **Implications Online.** The federal dilution statute provides trademark owners with a stronger remedy against those who own similar domain names, while potentially placing at risk those domain names owned by companies in noncompetitive industries. *See infra* § III(C). The law places a premium on registering marks, since a defendant's ownership of a registered mark on the principal register provides an absolute defense (while ownership of an unregistered mark does not).

C. Internet Domain Names

Domain names identify host computers for email and websites addresses. Domain names typically are comprised of an abbreviation, name or acronym, followed by a period and one of five world-wide generic top level domain categories (*.com* for commercial entities, *.edu* for educational institutions, *.org* for non-profit organizations, *.gov* for governmental entities, and *.net*) or country code domains (such as *.ca* for Canada or *.au* for Australia).

The Domain Name System (DNS) provides the mechanism for converting domain names into IP addresses and then back again. The modern domain name system, which was adopted in January 1986, was developed in 1983 by Paul Mockapetris, Craig Partridge and Jon Postel to accommodate increased use, and offered a tree-branch hierarchy of domain names emanating from seven top-level domains (TLDs): *.edu, .com, .org, .gov, .mil, .net, .int* (for international organizations), as well as country domains. Today, the Domain Name System is under the authority of the Internet Assigned Numbers Authority (IANA), which has delegated the operational Internet Registry to InterNIC (the Internet Network Information Center). InterNIC currently administers domain names registered in the *.com, .edu, .net* and *.org* TLDs. The U.S. Federal Networking Council is responsible for registrations in the *.gov* TLD, and has delegated that authority to InterNIC. Nicholas R. Trio, "What's in a Name?," OnTheInternet, Sept./Oct. 1996, at 20, 21, 22.

InterNIC has delegated responsibility for registering domain names in the worldwide generic top

level domains to Network Solutions, Inc. of Herndon, Virginia. Prior to October 1, 1995, domain names were assigned, free of charge, on a first-come, first-served basis. Since October 1995, InterNIC has charged registration and maintenance fees for domain names in the *.com, .org, .net, .edu* and *.gov* domains. David M. Graves & Robert McCollum, Fee for Registration of Domain Names, URL ftp://rs.internic.net/policy/ internic/internic-domain-3.txt (Sept. 14, 1995). Other registrars now also register generic top-level domain names (and have established their own dispute policies).

1. **Lack of vigilance by trademark owners.** For sound business reasons, most companies choose domain names that are readily associated with their trade names. Many companies which otherwise are vigilant about protecting their trademark rights, however, did not act quickly to reserve the domain name equivalent of their trademarks.

a. **mcdonalds.com.** The domain name *mcdonalds.com* was registered by a *Wired* magazine editor (Joshua Quittner), not McDonald's Corp. Joshua Quittner, "Billions Registered," Wired, Oct. 1994. Quittner subsequently sold the domain name to McDonald's. Richard Raysman & Peter Brown, "On-Line Legal Issues," N.Y.L.J., Feb. 15, 1995, at 3.

b. **mci.com.** Sprint initially was allowed to register the domain name *mci.com.* Joshua Quittner, "Billions Registered," *Wired,* Oct. 1994.

c. **kaplan.com.** Kaplan Education Centers discovered that the Internet domain name *kaplan.com* was registered by one of its rivals, Princeton Review, Inc. In arbitration over rights to the domain name *kaplan.com*, the arbitrators ruled that Princeton Review, Inc. had to relinquish the domain name but denied Kaplan's request for damages. Richard Raysman & Peter Brown, "On-Line Legal Issues," N.Y.L.J., Feb. 15, 1995, at 3.

2. **Over-registration**. While two-thirds of the Fortune 500 companies had not registered an obvious version of their trade names as domain names as of October 1994, by 1995 some companies had attempted to register hundreds of potential names. For example, Kraft/ General Foods registered 150 domain names and Proctor & Gamble Co. registered 200, including *badbreath.com, dandruff.com, diarrhea.com* and *underarm.com*. D. Krivoshik, "Paying Ransom on the Internet," N.J.L.J., Oct. 23, 1995, at 10.

3. **Early litigation over rights in domain names.**

a. ***MTV Networks v. Curry,*** 867 F. Supp. 202 (S.D.N.Y. 1994). Former MTV video disc jockey Adam Curry, while still employed by MTV, developed an Internet service with the Internet site address *mtv.com.* Curry alleged that he developed the Internet site independently of MTV, at his own expense, and with the express knowledge and support of MTV, which announced the mtv.com address on MTV Network broadcasts. By the spring of 1994, Curry's mtv.com address had been accessed by millions of Internet users. When MTV sought to launch its own service via America Online, it sued Curry for trademark infringement. Curry counterclaimed for breach of contract, fraud and negligent misrepresentation. The case settled in March 1995, with Curry relinquishing *mtv.com* to MTV. "MTV, Curry Settle," Information Law Alert, Mar. 24, 1995.

b. ***Council of Better Business Bureaus, Inc. v. Sloo.*** In May 1995,

the Council of Better Business Bureaus brought suit against Mark Sloo, an individual who registered the domain names *bbb.com* and *bbb.org,* and Tyrell Corp., Sloo's Internet service provider. "BBB" has been used as a trademark by the plaintiff for 32 years.

c. ***Fry's Electronics, Inc. v. Octave Systems, Inc.*** Fry's Electronics, Inc., a popular Silicon Valley electronics retail chain, brought suit in federal court in San Francisco in July 1995 over rights to the domain name *frys.com,* which had been registered by a Seattle fast food business known as Frenchy Frys. Octave Systems, Inc., Frenchy Frys' Internet provider, and NSI were named as defendants in the suit, which was brought for trademark infringement, unfair competition and RICO. "Spud Vendor's E-mail Address Prompts RICO Suit," The Recorder, Aug. 1, 1995, at 3; CyberLex (Aug. 1995).

d. ***KnowledgeNet, Inc. v. Boone.*** In December 1994, KnowledgeNet, Inc., a computer networking and consulting shop, brought suit in federal court in Chicago against David Boone, a Virginia business consultant who had registered *knowledgenet.com* as the domain name for a fledgling association of business consultants that Boone had formed to create a virtual networking circle in which independent consultants would make referrals and generate leads through email. Boone agreed to settle the case on fairly onerous terms after incurring in excess of $10,000 in legal fees. "Retreat and Surrender: Internet Trademark Suit Fizzles," Information Law Alert, July 7, 1995; "KnowledgeNet v. David Boone," Information Law Alert, May 12, 1995.

e. ***Wired v. Wire.*** Wired magazine, which owns the domain name *wire.com,* sued WIRE, a California computer network devoted to women's issues, which had registered *wire.net.* The case settled in 1995. Computer Litigation Journal, Vol. IV, No. 3, Oct. 1, 1995, at 12-13, *citing* The National Law Journal, May 8, 1995, at C37.

4. **Trademarks as domain names.** Trademark rights typically are recognized in a narrow class of goods. Different companies therefore may hold similar marks in different industries. For example, "Delta" is the trade name used by an airline and the manufacturer of household faucets. If Delta Airlines selected the domain name *delta.com* it would block the faucet manufacturer from using its trade name as its domain name, but would not have committed trademark infringement. If a company uses a domain name to trade on the good will associated with another company, however, a trademark or unfair trade claim could be brought.

5. **NSI's 1995 Domain Dispute Resolution Policy Statement.** In July 1995, Network Solutions, Inc. ("NSI") issued a policy statement to limit potential abuses of the domain name registration system and resolve conflicts where more than one party claims rights to a given domain name. NSI Domain Dispute Resolution Policy Statement, URL ftp://rs.internic.net/policy/internic/internic-domain-1.txt (July 1995). The Policy Statement was revised effective November 23, 1995, in part to delete the word "resolution" from the title of the Domain Dispute Policy Statement. URL ftp://rs.internic.net/ policy/internic/internic-domain-4.txt (Oct. 23, 1995). In the Policy Statement, NSI states that it "has neither the legal resources nor the legal obligation to screen requested Domain Names to determine if the use of a Domain Name by an Applicant may infringe upon the right(s) of a third party."

a. **Reservation of names.** To discourage acquisition of domain names to block future registrants, applicants must certify that they have a bona fide intention to use the domain name on a regular basis

on the Internet and that the proposed name "does not interfere or infringe the right of any third party in any jurisdiction with respect to trademark, service mark, trade name, company name or any other intellectual property right . . . ." Further, at the time of the initial submission of a domain name request, an applicant is "required to have operational name service from at least two operational Internet servers for that domain name." In addition, NSI reserves the right to force a registrant to relinquish any domain name that is not regularly used during any given 90-day period.

b. **Trademark infringement.**

(1) **Withdrawal of domain names.** The Policy Statement provides that NSI shall have the right to withdraw a domain name from use or registration on the Internet if it is presented with an order from a United States court or an arbitration panel chosen by the parties that a domain name rightfully belongs to a third party.

(2) **Dispute where third party does not own a registered trademark**. Where a dispute arises over a domain name registration, but the third party objector does not have a registered trademark or service mark in the same name, NSI will allow the applicant to use the contested domain name unless and until NSI receives a court order or arbitrator's award determining that the name rightfully belongs to the objecting party. Policy Statement 6(b).

(3) **Dispute based on third party's registered mark.** Where a third party's claim is based on a registered trademark or service mark:

(a) **If the applicant also owns a registered mark in the same name or shows first use of the domain name** (prior to the earlier of (a) the date of first use of the objector's trademark or service mark or (b) the effective registration date of the objector's mark): The applicant shall be allowed to continue using the contested name (provided it agrees to post a bond and indemnify NSI for any liability relating to the registration or use of the domain name), unless or until NSI is presented with a court order or arbitrator's award determining that the domain name rightfully belongs to the objecting party. Policy Statement 6(c)(1), 6(c)(2).

(b) **No registration or first use.** If the applicant does not present evidence of first use of the domain name or that it owns a registered mark, NSI will assign a new domain name to the applicant and allow the applicant to maintain both names simultaneously for up to 90 days to allow

an orderly transition to the new domain name. At the end of the transition period, NSI will place the disputed name on "Hold" status pending resolution of the dispute. Where the applicant refuses to accept assignment of a new domain name or relinquish its use of the disputed domain name, NSI will simply place the disputed name on "Hold" without allowing for a transition period. As long as a domain name is on "Hold," no other person or entity will be allowed to register that name. Policy Statement 6(c)(3), 6(c)(4).

(4) **Bond.** If eligible to continue with the disputed domain name, the applicant will be required to post a bond sufficient to cover claimed damages, or else the domain name will be placed on "Hold" status.

(5) **Definition of "registered trademark.**" for purposes of the Policy Statement, a "registered trademark" means "a valid and subsisting foreign or United States federal registration of a trademark or service mark that is in full force and effect . . ." State trademark or service mark registrations are expressly excluded.

c. **Indemnification.** The Policy Statement obliges registrants to indemnify NSI, the National Science Foundation, the Internet Assigned Numbers Authority (IANA), the Internet Activities Board (IAB) and the Internet Society for liability related to the applicant's use or registration of a domain name.

d. **Arbitration.** The Policy Statement provides that any dispute with NSI shall be subject to binding arbitration by the American Arbitration Association in San Diego, California, subject to the provisions of the California Evidence Code and the substantive law of California (excluding California's choice of law rules). No discovery shall be permitted.

e. **Results of the 1995 policy.** In the first six weeks after NSI adopted its new policy, domain name registrations dropped from 5,000 per week to about 1,300 per week. Edupage, Oct. 17, 1995, *citing* Investor's Business Daily, Oct. 17, 1995, at A10.

f. **Fees.** Effective October 1, 1995, NSI began charging $100 per new registration and $50 per year to maintain domain names in the *.com, .org, .net, .edu* and *.gov* domains. The current fee is $70 for a 2 year period.

6. **Litigation arising out of NSI's 1995 Domain Dispute Policy Statement.**

a. ***Roadrunner Computer Systems, Inc. v. Network Solutions, Inc.,*** Civil Action No. 96-413 (E.D. Va. Mar. 26, 1996). Roadrunner Computer Systems, Inc. ("RCS") brought suit against NSI for breach of contract, detrimental reliance and intentional interference with contractual relations arising out of NSI's adoption of its Domain Dispute Policy Statement. Plaintiff registered the domain name

roadrunner.com in 1994 under NSI's former "first come, first-served" policy. Time-Warner, owner of the "Road Runner" [two words] trademark for the cartoon character used on plush toys and other goods, challenged plaintiff's domain name registration under NSI's 1995 Domain Dispute Policy Statement. RCS argued that Time-Warner's trademark in "Road Runner" was not identical to RCS's domain name *roadrunner.com* and that the marks were not used in competition with one another (since RCS operated an Internet-related service, and Time-Warner used its mark on toys). RCS also argued that it had been using its domain name for more than a year and had over 500 customers who relied on it for Internet access. When NSI rejected these arguments, RCS obtained a trademark registration for the mark *roadrunner.com* in Tunisia, "a country selected because it grants trademark registrations quickly." Under NSI's Domain Dispute Policy Statement, RCS's submission of a valid trademark registration would have allowed RCS to post a bond and retain use of roadrunner.com pending a judicial or arbitral determination of its rights. When NSI rejected RCS's submission of its trademark registration as untimely, RCS brought suit. The case ultimately was settled.

b. **Clue.com.**

(1) ***Clue Computing, Inc. v. Network Solutions, Inc.,*** Case No. 96 CV 694 (Boulder Cty., CO. June 12, 1996). Clue Computing, Inc. ("CCI"), a Colorado Internet access provider, registered the domain name *clue.com* in June 1994. In February 1996, Hasbro, Inc., owner of the registered trademark "Clue," used in conjunction with a board game, filed a copy of its registered trademark with NSI, challenging CCI's domain name registration. CCI sought unsuccessfully to negotiate a resolution of the dispute with NSI and Hasbro. With a deadline pending for clue.com to be placed on hold status, CCI filed suit against NSI in state court in Boulder for breach of contract, detrimental reliance, intentional interference with contractual relations (based on CCI's contracts with customers, whose email addresses are tied to the *clue.com* domain name) and a declaratory judgment that NSI's 1995 Policy Statement could not be applied retroactively to CCI. Anticipating the defenses actually raised by NSI in *Roadrunner Computer Systems, Inc. v. Network Solutions, Inc.,* CCI alleged that NSI, in implementing its contract with the National Science Foundation pursuant to 31 U.S.C. § 6305, was obliged to act fairly and in an even-handed manner, but in fact acted arbitrarily and capriciously.

(2) ***Network Solutions, Inc. v. Clue Computing,*** Case No. 96-CV-694, (D. Colo. June 21, 1996). Instead of focusing its attention on CCI's state court action, NSI, on June 21, 1996, filed an interpleader action in federal court against Clue Computing, Inc. ("Clue") and Hasbro, Inc. ("Hasbro"), asking the court to determine which party should own *clue.com.* NSI refrained from placing CCI's domain name on hold, pending litigation.

c. ***Giacalone v. Network Solutions, Inc.,*** Case No.

96-20434 (N.D. Cal. June 14, 1996). Chicago-based Ty Inc., a manufacturer of toys, filed a complaint with NSI based on Philip Giacalone's registration of the domain name *ty.com*, a name that Giacalone, a web page designer, had selected because his son's name is Ty. Under NSI's Domain Policy Statement, Ty Inc., as the registered trademark owner, would have been entitled to have Giacalone's domain name placed on hold status pending resolution of the dispute, unless Giacalone could have produced evidence that he also owned a registered trademark in the name "Ty," which he was unable to do. Instead, after receiving a letter from NSI dated May 6, 1996, asking him to present NSI with evidence that he owns a registered mark in "ty" or agree to relinquish the ty.com domain name (and warning him that his failure to do either, would result in ty.com being placed on hold), Giacalone filed suit on May 30, 1996 alleging that Ty Inc. was attempting a "reverse domain name hijacking," and seeking a declaration that *ty.com* does not infringe Ty Inc.'s trademark, damages for intentional interference with advantageous business relationships, and cancellation of Ty Inc.'s mark based on trademark misuse. On June 14, 1996, just days before resigning from the bench, Judge Robert Aguilar entered a preliminary injunction prohibiting Ty Inc. from interfering with Giacalone's use of the *ty.com* domain name pending a final judgment, and ordering it to take "all steps necessary to see that Plaintiff's right to use the domain name *ty.com* is undisturbed and not suspended or interfered with in any way. . ." Although NSI is not subject to the preliminary injunction (based on its stipulation to abide by whatever order the court entered), the practical effect of the order prohibiting Ty Inc. from obtaining relief under NSI's Policy Statement was to enjoin NSI from implementing the 1995 Policy Statement in this case.

d. ***The Comp Examiner Agency, Inc. v. Juris, Inc.,*** Civil Action No. 96-0213 WMB (C.D. Cal. Apr. 23, 1996). Juris, Inc., the manufacturer and distributor of law office automation software and owner of the registered trademark "JURIS," obtained a preliminary injunction against The Comp Examiner Agency's use of the domain name juris.com to provide legal services because of a likelihood of consumer confusion. In its First Amended Counterclaim, Juris, Inc. had alleged that NSI failed to place *juris.com* on hold status, pursuant to its Domain Dispute Policy Statement (supra § III(C)(5)), after Juris, Inc., presented evidence that it owns the federally registered mark "JURIS" and plaintiff failed to respond to InterNIC's inquiry.

e. ***Avon Products v. Carnetta Wong Associates.*** Avon brought suit for trademark dilution (supra § III(B)) against Carnetta Wong Associates ("CWA"), which registered avon.com in 1995. While the suit was still pending in

federal court in the Eastern District of New York, Avon was successful in convincing NSI to rescind the registration for *avon.com* after CWA transferred it to David Lew two days before the litigation was instituted. Avon convinced NSI that the registration should be rescinded because CWA and Lew had violated NSI's policy, which requires applicants to affirm that a proposed registration does not violate a third party's trademark or other intellectual property or otherwise interfere with a third party's business. "Avon Retrieves Domain from Name Hijacker," Information Law Alert, Apr. 5, 1996.

7. **Domain names as trademarks.** In the first edition of this outline, it was predicted that: "In the future, as more people come on-line, and companies more actively use email for marketing purposes, it is likely that companies will advertise their domain names and some will claim trademark protection in those names." The PTO has since taken the position that Internet domain names may be registered if used as trademarks.

8. **1996 Domain Dispute Policy Statement.**

NSI's 1996 amended Policy Statement was intended, in part, to avoid cases such as *Roadrunner Computers Systems, Inc. v. NSI.* The Policy Statement shifted the burden to resolve domain name disputes almost entirely to U.S. courts in part to minimize litigation in which NSI is named as a defendant.

a. **Hold procedures.** The basic procedures for having a domain name placed on "hold" remained the same, except that the circumstances under which an order would issue were greatly reduced. Under Section 6(c) of the 1996 Policy Statement, a federal trademark registration obtained after a dispute had arisen would no longer provide grounds for obtaining (or avoiding) an NSI "hold" order. Thus, a domain name owner could not be able to quickly obtain a *foreign* federal trademark registration when it is notified by a U.S. trademark owner - or NSI - of a dispute over its domain name, as the plaintiff did in *Roadrunner Computer Systems, Inc. v. Network Solutions, Inc.*

b. **Definition of "registered."** The 1996 policy continued to afford preferential treatment to owners of *registered* trademarks, but with a new twist. For U.S. marks, only those registrations listed on the principal register could be used to obtain (or block) "hold" orders. U.S. marks registered on the supplementary register, which may be challenged as unprotectable in court, are, together with common law marks and intent to use applications, entitled to no priority. The Policy Statement continued to treat federally registered *foreign* trademarks on a par with U.S. registrations, regardless of whether such marks were incontestable in the country where they issue.

c. **Interpleader-style action.** Section 7 of the 1996 Policy Statement provided that NSI would not place a domain name on "hold" if either the domain name owner or the trademark owner first initiated litigation. In such cases, NSI will "deposit control of the domain name into the registry of the court" (Policy Statement 7(a)), or effectively respond as it did in the clue.com case

d. **Court order binding.** NSI stated that it would abide by any

temporary or final court order (AAA arbitration decisions were no longer given equal priority) so long as NSI itself were not joined in the litigation. If named as a party to a domain name lawsuit, the 1996 Policy Statement provided that NSI "shall not be limited to the above actions, but reserves the right to raise any and all defenses deemed appropriate." Policy Statement 7(c).

9. **The 1998 Policy Statement.** NSI modified its 1996 Policy Statement effective February 25, 1998. Domain Name Dispute Policy (Rev. 03), **http://rs.internic.net/domain-info/nic-rev03.html**.

a. **Registration on the principal registry "or equivalent registry" required.** Challenges based on foreign registrations must now be from registries "equivalent" to the U.S. principal registry.

b. **Litigation freezes the status quo ante.** Whereas under the prior policy the initiation of a lawsuit could prevent a domain name from being placed on hold, under the 1998 Policy Statement litigation merely freezes the status quo. Thus, a late-filed lawsuit filed by a domain name owner whose name has been placed on hold will not revive the name.

c. **Foreign lawsuits will stay NSI action.** Under the 1996 Policy Statement, only litigation in a U.S. court stayed further action. By changing the requirement to "a court of competent jurisdiction," NSI expressly recognized the authority of foreign courts to adjudicate rights in domain names it administers. See Policy Statement § 10(a).

10. **Domain Name Dilution.**

Owners of famous trademarks potentially have a potent remedy in domain name disputes in the form of the federal antidilution statute enacted in 1996. *See supra* § III(B). Among other things, dilution may be shown by evidence of blurring or tarnishment.

a. **Blurring.** Dilution may be shown by blurring. *See, e.g., I.P. Lund Trading ApS & Kroin, Inc. v. Kohler Co.,* 163 F.3d 27, 49-50 (1st Cir. 1998).

b. **Tarnishment.** Tarnishment typically is shown when a famous mark is associated with hard core pornography, spamming or cybersquatting.

(1) ***Hasbro, Inc. v. Internet Entertainment Group Ltd.,*** Case No. C96-139 (W.D. Wash. Feb. 5, 1996). In a suit brought by Hasbro, Inc., which owns the trademark "Candy Land," Judge Dwyer enjoined the defendant's use of the domain name candyland.com for a sexually explicit Internet site, under the Federal Trademark Dilution Act and Washington state's anti-dilution statute. In addition to *candyland.com,* the defendant had reserved the domain name *parkerbrothers.com,* which plaintiff's counsel argued evidenced the defendant's intent to trade on plaintiff's wholesome image as the manufacturer of board games for children. "Washington Judge Enjoins Use of Trademark as Internet Domain Name," Mealey's Litigation Reports: Intellectual Property,

Mar. 18, 1996.

(2) In ***Toys R Us v. Akkaoui***, Case No. C 96-3381 CW, 1996 U.S. Dist. LEXIS 17090 (N.D. Cal. Oct. 29, 1996) plaintiff Geoffrey Inc., owner of a family of marks ending in "R Us" (including Toys R Us, in use since 1960, and Kids R Us, in use since 1983) brought suit against Mohamad Ahmad Akkaoui, Lingerienet and Acme Distributors, which operated an Internet service offering sexual devices and clothing under the *adultsrus.com* domain name and Adults R Us mark. In entering a preliminary injunction, Judge Claudia Wilken of the Northern District of California determined that plaintiff's marks are distinctive and famous and that defendants' use of Adults R Us was likely to tarnish plaintiff's marks by associating them with sexual goods inconsistent with the wholesome image plaintiff sought to cultivate in the marketplace. *But see Toys "R" Us, Inc. v. Feinberg,* 26 F. Supp. 2d 639 (S.D.N.Y. 1998) (holding that the use of the gunsrus.com domain name by a Massachusetts gun dealer on a website entitled "Guns Are We" neither tarnished nor blurred plaintiff's marks), *rev'd on procedural grounds,* 201 F.3d 432 (2d Cir. 1999).

(3) In ***America Online, Inc. v. IMS,*** 24 F. Supp. 2d 548, 552 (E.D. Va. 1998), the court found that a famous mark could be diluted when used as a phony return email address in connection with unsolicited commercial email (or spam).

c. **No dilution will be found where a competing use does not diminish the value of a mark.** *See Hasbro, Inc. v. Clue Computing, Inc.,* 66 F. Supp. 2d 117 (D. Mass. 1999).

11. **Cybersquatting.** A cybersquatter is an individual who intentionally registers a third party's trademark as a domain name in order to extract a payment from the trademark owner or prevent its use of the mark as a domain name.

a. In ***Panavision Int'l, L.P. v. Toeppen,*** 141 F.3d 1316 (9th Cir. 1998), the Ninth Circuit affirmed a lower court ruling entering summary judgment in favor of a trademark owner against cybersquatter Dennis Toeppen based on federal and state dilution claims.

b. In ***Avery Dennison Corp. v. Sumpton,*** 189 F.3d 868 (9th Cir. 1999), the Ninth Circuit rejected the district court's holding that defendants - who registered over 12,000 surnames as domain names (including *avery.net* and *dennison.net*), which they used to operate a business licensing "vanity" email addresses - were cybersquatters.

12. **Typographical errors.** Beginning in about 1997, cybersquatters began registering obvious typographical errors and common misspellings of recognized trademarks as domain names in order to divert traffic to alternative sites. A claim may be easier to assert successfully where someone has registered multiple misspellings or an obvious variation of a recognized mark.

a. ***PaineWebber, Inc. v. wwwpainewebber.com,*** No. 99-0456-A (E.D. Va. Apr. 1999) is a typical case, where injunctive relief was

entered against the owners of *wwwpainewebber.com* (with no period between "www" and "painewebber.com").

b. Many registrants provide phony contact information when they register domain names, making it difficult to track them down. ***Columbia Insurance Co. v. Seescandy.com,*** 185 F.R.D. 573 (N.D. Cal. 1999) is a case that discusses this problem and a plaintiff's need in such cases to subpoena customer information.

c. Out of frustration with the difficulties associated with identifying those responsible, some litigants have sought to bring *in rem* actions against the domain names themselves, although the success of such an action may be questionable. *See infra* § III(c)(16).

13. **Use in commerce.**

a. In order to maintain an action under the Lanham Act, a plaintiff must establish use of a mark in connection with the sale of goods or services in commerce (or a "commercial use in commerce" under the Dilution Act).

b. Cybersquatting - or the practice of registering a third party's trademark as a domain name to prevent the mark owner's use and/or sell it to the trademark owner - has been recognized as commercial use. *See Panavision Int'l, L.P. v. Toeppen,* 141 F.3d 1316 (9th Cir. 1998) (sale or arbitrage); *New York State Society of Certified Public Accountants v. Eric Louis Associates, Inc.,* 79 F. Supp. 2d 331 (S.D.N.Y. 1999) (traffic diversion).

c. In ***Brookfield Communications, Inc. v. West Coast Entertainment Corp.,*** 174 F.3d 1036 (9th Cir. 1999), the Ninth Circuit ruled that merely using a domain name as an email address did not constitute the use of a mark in connection with the sale of goods or services, at least under the facts of that case.

d. In ***Planned Parenthood Federation of America, Inc. v. Bucci,*** 97 Civ. 0629 (KMW) (S.D.N.Y. Preliminary Injunction entered Mar. 19, 1997), *aff'd mem.,* 152 F.3d 920 (2d Cir.), *cert. denied,* 525 U.S. 834 (1998), Judge Kimba Wood ruled that the defendant, a pro-life activist who was using the domain name *plannedparenthood.com* for a website on which he posted anti-abortion material, was using plaintiff's mark "in commerce," within the meaning of 15 U.S.C. §§ 1114 and 1125(a), and as a "commercial use in commerce" within the meaning of 15 U.S.C. § 1125(c). The court concluded that even though the defendant did not seek to earn any revenue from the website, he posted materials about a book entitled "The Cost of Abortion" there to help promote sales by the book's author. In addition, the court found significant the fact that defendant's website was part of an effort to promote a business he operated called "Catholic Radio," in connection with which he solicited funds and encouraged third parties to join him in abortion protests. Finally, the court concluded that defendant's use was commercial because his actions were designed to, and in fact did, harm plaintiff commercially. *See also Jews for Jesus v. Brodsky,* 993 F. Supp. 282 (D.N.J. 1998) (ruling for the mark owner on similar facts), *aff'd mem.,* 159 F.3d 1351 (3d Cir. 1998).

e. In ***HQM, Ltd. v. Hatfield,*** 71 F. Supp. 2d 500 (D. Md. 1999), the

court ruled that merely because a domain name is registered in the .com TLD does not mean it is being used for a commercial purpose.

f. In ***OBH, Inc. v. Spotlight Magazine, Inc.,*** 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of *thebuffalonews.com* domain name for a parody site constituted a use in commerce because the site included links to defendant's other sites.

14. **What constitutes likelihood of confusion in Cyberspace.**

a. Initial interest confusion.

(1) In ***Interstellar Starship Services, Ltd. v. Epix Inc.,*** 184 F.3d 1107 (9th Cir. 1999), the Ninth Circuit ruled that likelihood of confusion may be established in cyberspace merely based on initial confusion (even if such confusion may be clarified once a visitor reaches an unintended site). *See also New York State Society of Certified Public Accountants v. Eric Louis Associates, Inc.,* 79 F. Supp. 2d 331 (S.D.N.Y. 1999). This doctrine is not yet universally recognized.

(2) In ***The Nashville Network v. CBS, Inc.,*** Case No. CV 98-1349 NM (ANx), 2000 U. S. Dist. LEXIS 4751 (C.D. Cal. Jan. 16, 2000), Judge Norma Manella ruled that initial interest confusion had to be evaluated by a "reasonably prudent consumer" standard, which could not be established in the case of *tnn.com* where the mark and domain name owners were not competitors. In this case, the court found significant the fact that the mark owner knew about the domain name registration several years before it initiated litigation.

b. In ***Data Concepts, Inc. v. Digital Consulting, Inc.,*** 150 F.3d 620 (6th Cir. 1998), the Sixth Circuit reversed an order granting summary judgment where the district court failed to consider the number of other websites using "DCI" in their domain names in evaluating likelihood of confusion.

c. No likelihood of confusion was found in ***Hasbro, Inc. v. Clue Computing, Inc.,*** 66 F. Supp. 2d 117 (D. Mass. 1999), where the defendant used *clue.com* as the domain name for an ISP service and there was no suggestion that it chose the name in order to trade on plaintiff's mark (used in connection with a children's board game).

d. **Case-sensitive domain names.** In ***CD Solutions, Inc. v. Tooker,*** 15 F. Supp. 2d 986 (D. Ore. 1998), the owner of mark "CDS" (Commercial Documentation Services) was not permitted to expand the scope of its mark to incorporate *cds.com,* which was used by the defendant to sell CD-ROMs.

15. **Registrars' duties to trademark owners.** *See supra* § III (A)(5).

16. ***In rem*** **actions to recover domain names.** Trademark owners hampered in their ability to locate and sue multiple, pseudonymous or overseas registrants, have attempted to bring in rem actions seeking a declaration of rights with respect to the domain names themselves. Such relief generally only may be obtained under the

Anticybersquatting Consumer Protection Act. *See infra* § III (D).

a. In ***Umbro Int'l, Inc. v. 3263851 Canada, Inc.,*** Record No. 991168, 2000 Va. LEXIS 75 (Va. Apr. 21, 2000) the Virginia Supreme Court ruled that a domain name registration is a contract right, not property, and therefore was not subject to garnishment under Virginia law.

b. In a similar action - ***Porsche Cars North America, Inc. v. Porsch.com,*** Civil Action No. 99-0006-A, 1999 U.S. Dist. LEXIS 8750 (E.D. Va. June 8, 1999) - a federal court in Virginia ruled that an *in rem* action to cancel a domain name registration could not be maintained under the Federal Trademark Dilution Act because that statute merely authorizes in personam proceedings.

c. In ***Dorer v. Arel,*** No. 98-266-A (E.D. Va. Sept. 3, 1999), a federal court ruled that a domain name registration is merely a contract right, rather than property subject to attachment or levy.

17. **ICANN's uniform domain name dispute resolution policy.** On October 24, 1999, ICANN approved its first Uniform Domain Name Dispute Resolution Policy, which would significantly change available extra-judicial remedies. A copy of the policy may be obtained at **http://www.icann.org/udrp/udrp-policy-24oct99.htm**. Unlike NSI's policy, domain names will no longer be placed on "hold" in response to complaints lodged by owners of registered trademarks that are identical to a third party's domain name. Rather, any complainant which claims trademark rights in a name that is identical or *confusingly similar* to a domain name (whether or not it owns a federal registration) may initiate a complaint which will be resolved by mandatory administrative dispute resolution (conducted by third party providers), agreement of the parties or litigation. In lieu of a "hold" order, relief to a successful complainant will result in an order canceling, suspending or transferring a domain name. In order to initiate a complaint with a registrar, however, a mark owner must allege that a domain name was registered and is being used in bad faith; "reverse domain name hijacking" or similar cases could no longer be addressed through extra-judicial administrative remedies. In addition, relief appears to be unavailable in cases where a domain name is registered but not used.

D. The Anticybersquatting Consumer Protection Act

1. **Bad faith registration, trafficking or use of a domain name.** The statute affords a private cause of action to the owner of a mark (including a personal name protected as a mark) if, without regard to the goods or services of the parties, a defendant (1) has a bad faith intent to profit from the mark; and (2) "registers, traffics in, or uses" a domain name that is:

- "identical or confusingly similar" to a mark that was distinctive at the time the domain name was registered;
- "identical or confusingly similar" to a mark that was famous at the time the domain name was registered; or
- is a "trademark, word or name" protected by 18 U.S.C. § 706 or 36 U.S.C. § 220506.

Bad faith may not be found if a court determines that a defendant "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful." The statute includes a nonexclusive list of factors that may be considered to evaluate whether "bad faith" exists within the meaning of the statute. Among other things, courts may consider--

- the trademark or other intellectual property rights of the person, if any, in the domain name;

- the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
- the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
- the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
- the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the good will represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the site;
- the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
- the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
- the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties;
- the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of 15 U.S.C. § 1125(c)(1).

15 U.S.C. § 1255(d)(1)(B)(i); *see also Sporty's Farm L.L.C. v. Sportsman's Market, Inc.,* Docket Nos. 98-7452(L), 98-7538(XAP), 2000 U.S. App. LEXIS 1246 (2d Cir. Feb. 2, 2000) (finding bad faith based on other grounds).

a. **Remedies**. Among other remedies, mark owners may obtain an order compelling a defendant to forfeit or transfer a domain name or cancel the registration. Injunctive relief and damages may be recovered on the same terms as otherwise are available under the Lanham Act.

b. **Statutory damages.** A plaintiff alternatively may elect special statutory damages of between $1,000 and $100,000 per domain name, set at an amount that "the court considers just," in lieu of actual damages and profits. This relief may be elected at any time prior to the entry of final judgment, but is only available for bad faith registration claims brought under 15 U.S.C. § 1125(d)(1). *See* 15 U.S.C. § 1117(d). The remedy of statutory damages - unlike other remedies under the statute - only applies to domain names registered on or after November 29, 1999.

2. ***In Rem* Relief.** The statute affords mark owners *in rem* relief against the domain name itself if the domain name violates the rights of the owner of a registered mark or a mark protected generally under the Federal Trademark Dilution Act or under section 1125(a) of the Lanham Act and a court expressly finds that the owner either was unable to obtain personal jurisdiction over the defendant or, through due diligence, was unable to find her by (1) sending a notice of the alleged violation and intent to proceed with an *in rem* action under the statute to the postal and email addresses provided by the registrant to a domain name registrar; and (2) publishing a notice of the action "as the court may direct promptly after filing the action." *See id.* § 1125(d)(2)(A).

a. **Remedies limited.** If an *in rem* action is brought, the statute limits a mark

owner's remedies to forfeiture or cancellation of the domain name or an order transferring it to the mark owner.

b. **Extra-judicial relief/Registrar Liability.** The statute also affords mark owners the opportunity to obtain extra judicial remedies from domain name registrars and registries in cases where *in rem* relief is sought. Specifically, upon receipt merely of "written notification" of a "filed, stamped copy of a complaint filed by the owner of a mark in a United States district court" any domain name registry, registrar or "other domain name authority" is required to: (1) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name; and (2) "not transfer, suspend, or otherwise modify the domain name during the pendency of the action" except to the extent ordered to do so by the court. Notwithstanding these obligations, domain name registrars, registries and other domain name authorities are exempted from liability for injunctive relief or damages "except in the case of bad faith or reckless disregard, which includes a willful failure to comply" with a court order.

c. **Constitutionality upheld.** The constitutionality of *in rem* relief under the statute was upheld in *Caesar's World, Inc. v. Caesar's - Palace.com,* Civil Action No. 99-550-A, 2000 U. S. Dist. LEXIS 2671 (E.D. Va. Mar. 3, 2000).

3. **Protection for the names of individuals.** The Act establishes a cause of action against persons who register a domain name that consists of the name of another living person (or a name substantially and confusingly similar) without the person's consent, "with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party . . ." Liability may not be imposed, however, where a domain name is registered in good faith and "is used in, affiliated with, or related to" a work protected under U.S. copyright law if the registrant is the copyright owner or a licensee, the person intends to sell the domain name in conjunction with the lawful exploitation of the work and the registration is not prohibited by any contract with the named person.

a. **Remedies.** Courts are authorized to award injunctive relief, including the forfeiture or cancellation of a domain name or its transfer to the plaintiff. Courts also are authorized, in their discretion, to award costs and attorneys' fees, to the prevailing party.

b. **Prospective application.** These special remedies only apply to domain names registered on after November 29, 1999. Individuals, however, also may obtain relief for bad faith registration, trafficking or use of a domain name pursuant to 15 U.S.C. § 1125(d)(1), which affords relief (although not statutory damages) for domain names registered prior to November 29, 1999. *See supra* § III (D)(1).

4. **Liability limitations for domain name registrars and registries.** The Act grants registries, registrars and others a blanket exemption from damages under the statute "for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name." As discussed above, other limitations also are created by the Act.

E. Trademark Liability for Metatag Infringement

Tags are HTML instructions in web pages that are not visible to visitors who access a site with a normal browser. Metatags are index words inserted in web pages so that the page will be identified when someone performs a search engine query for the word. In order to give greater prominence to a website when search engine queries are performed, some website developers

have inserted the same word multiple times in metatags (such as "ski ski ski ski ski ski" for a ski shop), so that a site may appear higher on a search engine list, or have included words otherwise unrelated to the site (such as the names of celebrities or sexual references) to increase the number of times the site is accessed. A number of suits have been filed over the use of trademarks as metatags in sites owned by third parties.

1. ***Brookfield Communications, Inc. v. West Coast Entertainment Corp.,*** 174 F.3d 1036 (9th Cir. 1999). The Ninth Circuit ruled that the unauthorized use of a trademark in metatags constituted trademark infringement.

2. ***Playboy Enterprises, Inc. v. Calvin Designer Label,*** Civil Action No. C-97-3204 CAL (N.D. Cal. preliminary injunction entered Sept. 8, 1997). Plaintiff, the owner of federally registered trademarks for PLAYBOY and PLAYMATE, sued defendants, who used the domain names *playboyxxx.com* and *playmatelive.com* to operate a website which included the names "Playmate Live Magazine" and "Get it all here @Playboy." Defendants were enjoined from using the PLAYBOY and PLAYMATE trademarks as

> Defendants' domain name, directory name, or other such computer address, as the name of Defendants' Web site service, in buried code or metatags on their home page or Web pages, or in connection with the retrieval or data or information or on other goods or services, or in connection with the advertising or promotion of their goods or services.

3. The defendant was found likely to prevail on her defense that using plaintiff's marks as metatags constituted a fair use in *Playboy Enterprises, Inc. v. Welles,* 7 F. Supp. 2d 1098 (S.D. Cal.), aff'd mem., Appeal No. 98-55911 (9th Cir. Oct. 20, 1998); *see infra* § III(H).

F. Key Words and Banner Advertisements

1. A key word is a term used in a search engine query. Many search engines sell the right to have a particular banner advertisement appear when a given key word is entered. For example, an automobile manufacturer might pay to have its advertisement appear whenever the word "car" was included in a query. According to one report, key word sales accounted for up to 25% of the revenue generated by top portal sites in 1998. *See* Greg Miller & Davan Maharaj, "Banner Ads on the Web Spark A Trademark Battle," L.A. Times, Feb 11, 1999.

2. Some (but not all) portal sites will sell third party trademarks as key words.

3. In ***Playboy Enterprises, Inc. v. Netscape Communications, Inc.,*** 55 F. Supp. 2d 1070 (C.D. Cal.), aff'd mem., 202 F.3d 278 (9th Cir. 1999), a court in Los Angeles held that Playboy was not likely to prevail on its Lanham Act claim against Excite and others based on the fact that Excite had sold two Playboy trademarks as part of a group of 450 words sold to third party advertisers. The court's opinion relied in large part on the questionable conclusion that the words "playboy" and "playmate" are English language words that do not suggest sponsorship or endorsement by any particular company.

4. A parallel action brought by Estee Lauder, Inc. against The Fragrance Counter currently is pending in the Southern District of New York. *See Estee Lauder, Inc. v. The Fragrance Counter, Inc.,* Case No. 1:99 cv 00382 (S.D.N.Y. complaint filed Jan. 19, 1999).

G. Trade Dress Protection for Screen Displays and Web Site Interfaces

1. In contrast to a trademark, trade dress refers to the "total image of a product" and

may include packaging, color combinations and graphics*. E.g., International Jensen v. Metrosound U.S.A.,* 4 F.3d 819, 822 (9th Cir. 1993), *citing Vision Sports, Inc. v. Melville Corp.,* 888 F.2d 609, 613 (9th Cir. 1989). Although broader rights may be recognized in a trade dress than a trademark, the legal standards governing trade dress protection are the same as for unregistered trademarks under section 43(a) of the Lanham Act. International Jensen, 4 F.3d at 823, citing *Two Pesos, Inc. v. Taco Cabana, Inc.,* 505 U.S. 763 (1992) ("section 43(a) provides no basis for distinguishing between trademark and trade dress"); *Rachel v. Banana Republic, Inc.,* 831 F.2d 1503, 1506 (9th Cir. 1987).

2. In evaluating whether trade dress protection is available, a court should compare factors such as the design and layout of the product, the graphics used, the background, including white graphics, packaging (including identical text found in both packaging), and similar factors. *E.g., Lisa Frank, Inc. v. Impact International, Inc.,* 799 F. Supp. 980 (D. Ariz. 1992).

3. **Functionality.** The functionality doctrine will bar trade dress protection for all but the most innovative and creative interfaces. "A product feature is functional if it is essential to the use or purpose of the article or if it affects the cost or quality of the article." *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.,* 456 U.S. 844, 851 n.10 (1982). Stated differently, "a design is legally functional . . . if it is one of a limited number of equally efficient options available to competitors and free competition would be unduly hindered by according the design trademark protection." *Two Pesos, Inc. v. Taco Cabana, Inc.,* 505 U.S. 763 (1992). However, elements that are separately functional, and hence unprotectable, may be combined and collectively entitled to trade dress protection. *E.g., Interactive Network, Inc. v. NTN Communications, Inc.,* 875 F. Supp. 1398, 1406 (N.D. Cal. 1995); *Lisa Frank, Inc. v. Impact International, Inc.,* 799 F. Supp. 980, 986 (D. Ariz. 1992).

4. **Timing may be critical.** Innovation in the software industry occurs at a very rapid pace. An interface that is fanciful today may become generic within a year, or even a matter of months. This is especially true of many applications programs. By contrast, the interfaces of creatively designed websites or videogame programs are more likely to be deemed protectable, even over time.

5. **Case law.** There are no reported website trade dress opinions and no recent, authoritative decisions upholding trade dress protection in a user-interface. Many companies, however, are attempting to protect the user-interfaces of their most creative programs as their trade dress, especially since the U.S. Supreme Court issued its decision in *Two Pesos, Inc. v. Taco Cabana, Inc.,* 505 U.S. 763 (1992), upholding the appearance of a Mexican restaurant as a company's trade dress.

> a. In ***Engineering Dynamics, Inc. v. Structural Software, Inc.,*** 26 F.3d 1335, 1350 (1994), *mod. on other grounds and reh'g denied,* 46 F.3d 408 (5th Cir. 1995), the Fifth Circuit upheld the trial court's rejection of plaintiff's trade dress infringement claim based on the trial court's determination that there was no likelihood of confusion between the two engineering programs at issue in that case. The Fifth Circuit noted in dicta that it was "an interesting question, unnecessary to reach here, whether computer input formats and output reports involving highly technical data are so inherently functional as not to be protectable." 26 F.3d at 1350 n.16.
>
> b. In ***Computer Care v. Service System Enterprises, Inc.,*** 982 F.2d 1063 (7th Cir. 1992), the Seventh Circuit upheld a finding of trade dress infringement based on defendant's wholesale copying of the layout of plaintiff's computer-generated sales brochure, reminder

letters and monthly reports, which were deemed to constitute an inherently distinctive trade dress. Although individual elements of the forms were functional, and hence unprotectable, the Seventh Circuit emphasized that plaintiff sought to protect "the overall format of each of its . . . reports, which Service Systems copied in their entirety." *Id.* at 1071. If the format and arrangement of the forms in *Computercare v. Service System Enterprises, Inc.* (which are shown on pages 1077 to 1085 of the opinion) are protectable as an inherently distinctive trade dress, then certain user interfaces similarly could be found to be protectable as a company's trade dress, and provide grounds for a trade dress infringement action in the Seventh Circuit, at least when copied exactly.

c. In ***Interactive Network, Inc. v. NTN Communications, Inc.,*** 875 F. Supp. 1398 (N.D. Cal. 1995) the user interface of an interactive video football game was held not to constitute a licensor's trade dress because the claimed features were functional.

d. In ***Brown Bag Software v. Symantec Corp.,*** No. 88 20352 (N.D. Cal. Nov. 10, 1992), *aff'd,* 29 F.3d 630 (9th Cir.), *cert. denied,* 513 U.S. 1044 (1994), Brown Bag Software's Lanham Act claim was rejected in large part on procedural grounds.

e. In M***idway Manufacturing Co. v. Dirkschneider,*** 543 F. Supp. 466, 484-90 (D. Neb. 1981), the court held that the plaintiff had shown probable success on the merits on its trade dress infringement claim based on the audiovisual display of plaintiff's video game. The court determined that the unique shapes and colors of plaintiff's video game characters were arbitrary embellishments, rather than being merely functional.

f. Recent decisions limiting the scope of copyright protection for nonliteral aspects (*i.e.,* the "look and feel") of a program (see supra § II(C)(3)(d)) are likely to renew interest in trade dress protection for screen displays.

6. The Internet's transformation of trade dress infringement claims. The argument that distinctive user interfaces should be entitled to trade dress protection is likely to be strengthened as more software becomes commercially available via the Internet. While attempts to protect the user interface of a computer program as a company's trade dress have been hampered by the fact that the interface is not necessarily the image projected by a company in its packaging or advertising, when software is sold via the Internet a much stronger argument can be made that the user interface itself is the protected trade dress. How courts will rule on this issue, however, remains to be seen.

H. Fair Use (Including Consumer Criticism and First Amendment Issues)

1. Fair use is a defense to a suit for infringement of an incontestable mark if the use is "otherwise than as a mark" or if the mark is used in good faith to describe the goods or services of a party or its geographic origin. 15 U.S.C. § 1115(b)(4); *New Kids on the Block v. News America Publishing, Inc.,* 971 F.2d 302 (9th Cir. 1992) (use of plaintiff's mark by newspapers to invite subscribers to call a 900 number dedicated to the musical group associated with the mark held to be a nominative fair use). Whether a commercial use of a mark is fair will depend upon whether (1) the allegedly infringing good or service is one not readily identifiable without use of the mark, (2) the mark is used only to the extent reasonably necessary to identify the

good or service, and (3) the user has not done anything to suggest, in conjunction with use of the mark, sponsorship or endorsement by the trademark holder. *E.g., Abdul-Jabbar v. General Motors Corp.,* 85 F.3d 407, 412 (9th Cir. 1996).

2. In addition, in a dilution claim brought under 15 U.S.C. § 1125(c) (or other cause of action under section 1125), any use of a mark deemed to be noncommercial, a form of news reporting or commentary or a fair use (of a famous mark) to identify another entity in comparative commercial advertising or promotion to identify competing goods and services, would not be actionable. 15 U.S.C. § 1125(c)(4).

3. In ***Playboy Enterprises, Inc. v. Welles,*** 7 F. Supp. 2d 1098 (S.D. Cal. 1998), *aff'd mem.*, Appeal No. 98-55911 (9th Cir. Oct. 20, 1998), the court denied plaintiff's application for a preliminary injunction against the former 1981 Playmate of the Year, in a case alleging trademark infringement and dilution based on her use of the "Playmate of the Year" title on her web page, "PMOY '81" as a watermark in the background of her website and the use of the "Playboy" and "Playmate" marks as meta tags. The court found that the defendant used plaintiff's marks truthfully to identify herself and therefore was likely to prevail in her fair use defense. *See also Playboy Enterprises, Inc. v. Terri Welles, Inc.,* Case No. 98-CV-0413-K(JFS), 1999 U.S. Dist. LEXIS 21047 (S.D. Cal. Dec. 1, 1999) (entering summary judgment in favor of the defendant).

4. The defendant also was found likely to prevail on its fair use defense in ***Bally Total Fitness Holding Corp. v. Faber,*** 29 F. Supp. 2d 1161 (C.D. Cal. 1998), which is a case that involved a "consumer criticism" site. Among other things, the court ruled that there was not likely to be confusion between plaintiff's genuine site and defendant's "BALLY SUCKS" website. *See infra* § IV(E)(4).

5. In ***OBH, Inc. v. Spotlight Magazine, Inc.,*** 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of *thebuffalonews.com* domain name for a parody site was not a fair use because a fair use parody depends on a lack of consumer confusion (which was not found in this case).

6. Whether use of a domain name is expressive - in which case it may be entitled to First Amendment protection - or merely serves a source-identifying function (in which case it is not) is analyzed in ***Name.Space, Inc. v. NSI,*** 202 F.3d 773 (2d Cir. 2000).

Next Section / Contents

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

IV. THE LAW OF CACHING, LINKING, FRAMING AND CONTENT AGGREGATION

A. Caching

1. **Definition.** Caching is the process of storing data on a computer, and therefore involves the creation of a protectable work under the Copyright Act. *MAI Systems Corp. v. Peak Computer, Inc.,* 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994); *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 907 F. Supp. 1361, 1378 n.5 (N.D. Cal. 1995).

2. Caching occurs at the server level (called proxy caching), when an on-line provider stores a popular site to facilitate quick linking or a company uses a proxy server for security reasons as part of a firewall. Browsers also "locally" cache, or store recently visited web pages in a computer's RAM. *See* Eric Schlachter, "Caching on the Internet," The Cyberspace Lawyer, Oct. 1996, at 2.

3. Unauthorized caching may constitute copyright infringement and, if protected trademarks are contained on the cached site, create potential liability for trademark infringement or unfair competition.

B. Hypertext Links

1. Definition. Hyperlinks allow a visitor to a site to easily and quickly connect to another location on the World Wide Web. A hyperlink is created by inserting a URL into HTML code, which then allows visitors to the website to point and click to a particular icon or portion of highlighted text and automatically access the linked site.

2. Linking compared to caching. To a user, there may be no practical difference between pointing and clicking on an icon that will connect to a linked website, and pointing and clicking on an icon that will call up a cached site. Unlike caching, however, linking does not involve the creation of a "copy" within the meaning of the Copyright Act except, arguably, when a viewer accesses a website (which causes a temporary copy of the site to be stored in the viewer's screen memory). A party establishing a link therefore could not be held liable for direct copyright infringement. In theory, a linking party might be subject to contributory or vicarious liability based on the infringing temporary copy created on a visitor's screen memory, although it would be difficult to make out such a claim. Potential defenses would include fair use and implied license.

3. Lanham Act Liability. Linking could create Lanham Act liability if the link created consumer confusion about the origin of a site or was unfair or deceptive. A deceptive content link could subject a party to liability. Most links that are not otherwise unfair - especially site links - would not give rise to a cause of action. Potential defendants might be able to assert fair use defenses available under the

Lanham Act.

C. Framing

1. Definition. Frames are a feature which, when used in conjunction with certain browsers, allow visitors to a website to view content from other sites without actually leaving the first page. Depending on how they are structured and the visitor's sophistication, frames arguably may make it difficult to discern content that is linked and run in frames from content that is original to the site. This is especially true because the framing site's URL remains displayed at the top of the screen, even while the other site is displayed. Framing is like linking only with an arguably greater opportunity for consumer confusion.

D. Copyright and Related Cases

1. In ***Shetland Times Ltd. v. Wills,*** Edinburgh, Scotland, Court of Session, Oct. 24, 1996 (Lord Hamilton), the Shetland Times Ltd. brought suit against Zetnews Limited and its managing director, Jonathan Wills, based on the content links established by the defendants to plaintiffs' website for the *Shetland Times* newspaper. Defendant created content links from its site to stories on plaintiff's website, which created the false impression that visitors were accessing news stories from defendants' newspaper, but which actually had been published in plaintiff's. Although widely cited on the Internet, the case has little legal significance in that it is an unreported decision (which under U.K. law has no precedential value) and turned on an interpretation of U.K. statutory law and was rendered without benefit of "detailed technical information . . . in relation to the electronic mechanisms involved." The court found that the plaintiffs had made a *prima facie* showing that the defendants' use of plaintiff's copyrighted headlines on their website constituted a violation of the of section 7 of the Copyright, Designs and Patent Act of 1988 (for which there is no U.S. corollary). The court rejected the argument, however, that the defendants were also liable for establishing the content link.

2. In ***Futuredontics, Inc. v. Applied Anagramics, Inc.,*** Appeal No. 97-565711 (9th Cir. July 6, 1998), the Ninth Circuit affirmed a district court ruling denying plaintiff's motion for a preliminary injunction in a case where the plaintiff alleged that the defendant created an unauthorized derivative work by framing plaintiff's website.

3. In ***Bernstein v. J.C. Penney, Inc.,*** Case No. 98 -2958 R (Ex) (C.D. Cal. granting defendants' motion to dismiss Sept. 29, 1998), celebrity photographer Gary Bernstein filed suit against the J.C. Penney department store and cosmetics company Elizabeth Arden alleging copyright infringement based on a link from a J.C. Penney site created in November 1997 to advertise Passion, an Elizabeth Arden perfume promoted by actress Elizabeth Taylor. A link from a portion of that site (which featured online chat with Elizabeth Taylor) led to a site hosted by Internet Movie Database, which maintained a site containing biographical information on Ms. Taylor. That site, in turn, contained links to several other locations - including a site run by Swedish University Network (SUNET) where unauthorized reproductions of two photographs that Mr. Bernstein had taken of Ms. Taylor were posted. In dismissing plaintiff's suit, Judge Manuel Real of the Central District of California implicitly ruled that the connection between defendant's site and the infringing photograph was too far removed to be actionable under the Copyright Act.

4. **Injunction granted based on contributory infringement.** In ***Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,*** 75 F. Supp. 2d 1290 (D. Utah 1999), the court entered an injunction prohibiting linking where defendants encouraged visitors to a website - via links - to access infringing content located elsewhere. The case involved more than mere linking, however. Defendants - after

being ordered to remove unauthorized copies of plaintiff's protected "Church Handbook of Instructions" from their website - created links to three other locations where infringing copies of the book could be accessed. They also posted emails on their site encouraging visitors to browse the linked locations, print copies of the handbook and email copies to third parties. Although the court concluded that plaintiffs had not shown that defendants contributed to the third party acts of infringement by the owners of the linked sites, it ruled that defendants actively encouraged individual users to infringe plaintiff's copyright by browsing the infringing sites (causing unauthorized temporary copies to be cached in a user's screen RAM) and printing or re-posting unauthorized copies on other websites. A different case would have been presented if the linked content was not infringing or if defendants had not actively encouraged third party acts of infringement.

5. A claim based on contributory copyright infringement was rejected in ***Ticketmaster Corp. v. Tickets.com, Inc.,*** CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000) - a case involving content (or "deep") linking - in which the court ruled in part that Ticketmaster's purported license restrictions prohibiting this practice were unenforceable because they were contained in Terms and Conditions which users were not actually required to review in order to access the Ticketmaster site.

E. Lanham Act and Related Cases

1. **Deep Linking.**

a. In ***Ticketmaster Corp. v. Microsoft Corp.,*** Case No. 97-3055 DDP (C.D. Cal. Complaint filed Apr. 28, 1997), Ticketmaster sued Microsoft for dilution, unfair trade under the Lanham Act and California state law, and declaratory relief relating to content links created from Microsoft's Seattle Sidewalk website to locations on Ticketmaster's site, use of Ticketmaster trademarks on the Seattle Sidewalk site, use of links and references to Ticketmaster to sell advertising on Microsoft's own site, and "misdescriptions" of Ticketmaster goods and services on the Seattle Sidewalk site. Microsoft filed a counterclaim seeking a declaration that the practice of linking websites does not violate U.S. law. The case settled in early 1999 with Microsoft agreeing not to provide any content (or "deep") links to Ticketmaster's site.

b. In ***Ticketmaster Corp. v. Tickets.com, Inc.,*** CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000) - the only ruling to date on the issue of content linking - Judge Harry L. Hupp granted the defendant's motion to dismiss, ruling that "deep linking by itself (i.e., without confusion of source) does not necessarily involve unfair competition." In so ruling, the court rejected Ticketmaster's contract and license-based arguments because users of its site were not actually required to review the site's Terms and Conditions.

2. **Framing.**

a. In ***The Washington Post Co. v. TotalNews, Inc.,*** Case No. 97 Civ. 1190 (PKL) (S.D.N.Y. Complaint filed Feb. 20, 1997), plaintiffs the Washington Post Co., Time Inc., Cable News Network, Inc., Times Mirror Co. d.b.a. The Los Angeles Times, Dow Jones & Co. and Reuters New Media Inc. brought suit in the Southern District of New York for common law misappropriation; federal trademark dilution; trademark infringement; false designation of origin, false

> representations and false advertising; trademark infringement and unfair competition under N.Y. Gen. Bus. L. § 368-e; state law dilution, pursuant to N.Y. Gen. Bus. L. § 368-d; deceptive acts and practices under N.Y. Gen. Bus. L. §§ 349-350; and copyright infringement. Defendants were the owners and operators of the totalnews.com website that ran plaintiff's websites in frames made to appear like different channels on a television set. The frames used by defendants cut off the borders on some of the websites, arguably devaluing the sites' content. Plaintiffs objected that defendants ran their own advertisements on a site dedicated exclusively to running third party news sites in frames. The case settled, with defendants agreeing to link - but not frame - plaintiffs' sites.

b. In ***Hard Rock Café Int'l Inc. v. Morton,*** 97 Civ. 9483, 1999 U.S. Dist. LEXIS 8340 (S.D.N.Y. June 1, 1999), the court ruled, in a case involving a trademark license, that the act of framing a website, under the facts of the case before it, was likely to cause consumer confusion. *See also Hard Rock Café Int'l (U.S.A.) v. Morton,* 97 Civ. 9483 (RPP), 1999 U.S. Dist. LEXIS 13760 (S.D.N.Y. Sept. 9, 1999).

3. In ***Playboy Enterprises, Inc. v. Universal Tel-A-Talk, Inc.,*** Civil No. 96-6961 (E.D. Pa. June 1, 1998), the court held that an unauthorized link to a website could not form the basis for a counterfeiting claim. In a later opinion, however, the court held that links from defendants' infringing "Playboy's Private Collection" website to Playboy's website evidenced that they adopted the "PLAYBOY" and "BUNNY" marks in an effort to capitalize on plaintiff's marks. *See Playboy Enterprises, Inc. v. Universal Tel-A-Talk, Inc.,* Civil Action No. 96-6961, 1998 U.S. Dist. LEXIS 17282 (E.D. Pa. Nov. 2, 1998) (permanently enjoining defendants from - among other things - "providing a link to Plaintiff's website 'Playboy.com.'").

4. In ***Bally Total Fitness Holding Corp. v. Faber,*** 29 F. Supp. 2d 1161 (C.D. Cal. 1998), a health club chain brought suit against an individual who operated a site entitled "Bally Sucks" as - what the court termed - a "consumer product review of Bally's services." The defendant did not use plaintiff's marks as part of the domain name for the site, although he did include them in metatags. At the outset of the lawsuit, the defendant included a link from the "Bally Sucks" site to "Images of Men," a site that he operated under the same domain name (compupix.com) that displayed and sold photos of naked men. This link subsequently was disabled. Among other rulings, the court expressly rejected the notion that an ordinary link to a pornographic site could create tarnishment:

> The essence of the Internet is that sites are connected to facilitate access to information. Including linked sites as grounds for finding commercial use or dilution would extend the statute far beyond its intended purpose of protecting trademark owners from uses that have the effect of "lessening . . . the capacity of a famous mark to identify and distinguish goods or services."

5. A different result obtained in ***Archdiocese of St. Louis v. Internet Entertainment Group, Inc.,*** 34 F. Supp. 2d 1145 (E.D. Mo. 1999), in which a court in St. Louis enjoined the defendant's operation of the *papalvisit.com* and *papalvisit1999.com* websites which, in addition to publicizing Pope John Paul's visit to St. Louis, included banner advertisements on virtually every page that were linked to adult websites. The sites also included off-color jokes about the Pope and the Catholic church. The court found that defendants' use tarnished (and therefore diluted) the Archdiocese's alleged common law marks in "Papal Visit 1999," "Pastoral Visit," "1999 Papal Visit Official Commemorative Items" and "Papal Visit

1999, St. Louis." The case was decided in part under Missouri's dilution statute, which does not require a showing that a mark is "famous."

6. In ***OBH, Inc. v. Spotlight Magazine, Inc.,*** 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of thebuffalonews.com domain name for a parody site constituted a use in commerce within the meaning of the Lanham Act because the site included links to defendant's other sites.

7. In ***Nissan Motor Co. v. Nissan Computer Corp.,*** 89 F. Supp. 2d 1154 (C.D. Cal. 2000), Judge Dean Pregerson entered a narrow injunction prohibiting the defendant from displaying automobile-related information, advertising or links (including links to automobile-related portions of Internet search engines) on its site. Uri Nissan, the owner of Nissan Computer Corp., had registered *nissan.com* for his business - Nissan Computer Corp. - in the mid-1990s. In the late 1990s, however, he sought to sell the domain name to Nissan Motor Co. and created links to car sites from his website. In enjoining these new uses, the court also ordered the defendant to include disclaimers identifying the owner of the Nissan Computer Corp. site and disclaiming any affiliation with Nissan Motor Co. (and providing the URL for that site).

F. Technological Self-Help. Links and frames may be effectively disabled in most cases.

G. The Digital Millennium Copyright Act. Liability for linking may be limited by complying with the Digital Millennium Copyright Act. *See supra* § II(G).

H. Content Aggregation.

1. Content aggregators - such as meta-search engines - aggregate material from other websites. In ***eBay, Inc. v. Bidder's Edge, Inc.,*** No. C-99-21200 RMW, 2000 U.S. Dist. LEXIS 7287 (N.D. Cal. May 23, 2000), eBay brought suit against an aggregator which allowed users to search multiple auction sites simultaneously, alleging copyright, Lanham Act and state law theories of recovery. Judge Whyte of the Northern District of California preliminarily enjoined the defendant from repeatedly accessing eBay's website based on a theory of trespass to chattels under California law. The defendant - Bidder's Edge - had repeatedly accessed eBay's site to copy content on a database, which was frequently updated but not as current as material actually found on eBay's site. In addition to lost capacity, the court deemed it significant that the defendant did not comply with guidelines established by eBay pursuant to the Robot Exclusion Standard.

2. **FTC Investigation.** The FTC presently is investigating eBay's licensing and litigation practices and their potential effect on consumer access to information.

3. In ***Storm Impact, Inc. v. Software of the Month Club,*** 13 F. Supp. 2d 782 (N.D. Ill. 1998), the court ruled that the defendant's practice of aggregating (free) shareware software from the Internet, which it sold as part of CD ROM compilations, constituted copyright infringement in violation of the terms of the plaintiff's shareware license.

4. In evaluating potential claims based on content aggregation (or "screen scraping"), courts may find significant factors such as (1) whether aggregators block content (including advertisements) from target sites; (2) whether content is aggregated in a way which disparages the reputation of a target site (for example, where stale or inaccurate information is presented); and/or (3) whether protected material is being copied in violation of copyright law.

I. **Visual Search Engine Practices.** *See supra* § II(E)(9).

Next Section / Contents

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

V. MISAPPROPRIATION OF TRADE SECRETS IN CYBERSPACE

A. Definition

1. **State law.** Trade secret protection is available by virtue of state law and therefore varies by jurisdiction. *See, e.g.,* Cal. Civil Code §§ 3426 to 3426.6. One of the best illustrations of this point was provided by the Texas Supreme Court in 1995, when it rejected the law in force in 39 other states and held that, under Texas law, the discovery rule does not apply to extend the statute of limitations period to bring misappropriation of trade secret claims. *Computer Associates Int'l v. Altai, Inc.,* 918 S.W.2d 453 (Tex. 1996).

2. **What is a trade secret?**

a. **Restatement of Torts**. The most common definition of a trade secret is found in the Restatement of Torts § 757: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."

b. **California statutory definition.** Cal. Civ. Code § 3426.1(d) defines a trade secret as:

> Information, including a formula, pattern, compilation, program, device, method, technique, or process that: (1) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

3. **Elements of a cause of action.**

a. **General principles.** To state a claim for misappropriation of trade secrets, generally a plaintiff must show that: (1) software or information incorporates a trade secret; (2) plaintiff took reasonable steps to preserve its secrecy; and (3) the defendant misappropriated the secret or used improper means, in breach of a confidential relationship, to acquire the trade secret. *E.g., Data General Corp. v. Grumman Systems Support Corp.,* 36 F.3d 1147, 1165 (1st Cir. 1994).

b. **A California cause of action.** Under California law, the following elements must be proven: (1) the information sought to be protected

must have independent economic value, actual or potential; (2) that independent economic value must be derived from not being generally known to the public or to other persons who can obtain economic advantage from its disclosure or use; (3) the information must be the subject of efforts that are reasonable under the circumstances to maintain its secrecy; (4) to be misappropriated, (a) a trade secret must be acquired by a person who knows or has reason to know that the trade secret was acquired by improper means (including theft and breach or inducement of breach of a duty to maintain secrecy) or (b) the trade secret must be used or disclosed by a person who knew or had reason to know that his knowledge of the trade secret was derived from a person who used improper means to acquire it or who owed a duty to the plaintiff to maintain its secrecy or (c) if the trade secret was acquired by accident or mistake, the acquirer knew or had reason to know that information before undergoing a material change of his position. Cal. Civ. Code §§ 3426.1(d)(1), 3426.1(d)(2), 3426.1(b).

B. Secrecy Required

1. **Disclosure destroys the secret.** The U.S. Supreme Court held that, "upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected." *Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470, 475-76 (1974).

2. **Modern standard: reasonable protection.** Generally, reasonable efforts to protect the secrecy of an alleged trade secret are all that is required. *See, e.g., Gates Rubber Co. v. Bando Chemical Industries, Ltd.,* 9 F.3d 823, 849 (10th Cir. 1993) (Colorado law). A limited disclosure, for a brief period of time, therefore may not necessarily defeat trade secret protection. *See id.*

3. **A company's failure to following its own procedures.** Although there are no "hard and fast" rules that companies must follow to protect their trade secrets, it is important that whatever policies are adopted are actually followed. A company's failure to follow its own procedures provides a basis for denying trade secret protection. *CVD, Inc. v. Raytheon Co.,* 769 F.2d 842 (1st Cir. 1985), *cert. denied,* 475 U.S. 1016 (1986).

C. Trade Secrets Posted over the Internet

Whether trade secret protection will be lost for information that was misappropriated and posted over the Internet should depend in part on how widely the information was disseminated. Simply because information theoretically may be available to millions of people online does not in fact mean that it was widely accessed (or accessed at all) if posted for a brief period of time at an obscure location or on an unpopular BBS. Three cases brought against former members of the Church of Scientology raise intriguing issues about the scope of trade secret protection in Cyberspace.

The Church of Scientology treats certain of its religious documents as trade secrets that it only discloses to advanced members, in a particular order and manner. In each case, former Scientology members posted confidential documents online and suit was brought against the former members and their Internet access providers.

1. In ***Religious Technologies Center v. Lerma,*** 897 F. Supp. 260 (E.D. Va. 1995), Judge Brinkema determined that church documents were not entitled to trade secret protection under Virginia law primarily because the documents "escaped into the public domain and onto the Internet." In a subsequent opinion, Judge Brinkema granted summary judgment in favor of the *Washington Post* defendants on plaintiffs'

misappropriation of trade secret claim based on his finding that the alleged trade secrets had been posted on the Internet on July 31 and August 1, 1995, and had remained available for more than ten days, until after a T.R.O. was entered on August 11, 1995, "where they remained potentially available to the millions of Internet users around the world." *Religious Technology Center v. Lerma,* 908 F. Supp. 1362 (E.D. Va. 1995). In support of her ruling, Judge Brinkema cited *Religious Technology Center v. Netcom On-Line Communication Services, Inc.,* 923 F. Supp. 1231 (N.D. Cal. 1995) (*infra* § V(C)(3)), writing that "[a]lthough the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet." 908 F. Supp. at 1368.

2. A similar result was reached in ***Religious Technology Center v. F.A.C.T.Net, Inc.,*** 901 F. Supp. 1519 (D. Colo. 1995), in which Judge Kane determined that Scientology documents were not entitled to protection under the Colorado Uniform Trade Secrets Act because "[d]espite RTC and the Church's elaborate and ardent measures to maintain the secretary of the Works, they have come into the public domain by numerous means . . . . The evidence also showed portions of the Works have been made available on the Internet . . . with the potential for downloading by countless users."

3. The same result also was reached in ***Religious Technology Center v. Netcom On-Line Communication Services, Inc.,*** 923 F. Supp. 1231 (N.D. Cal. 1995), which provides the most thorough analysis of the issue. Judge Whyte of the Northern District of California wrote that although the defendant could not rely on his own improper postings to support the argument that Scientology documents were no longer secret, evidence that others put the material into the public domain prevented plaintiff from further enforcing its trade secret rights in those materials. *Id.* at 1256. Judge Whyte concluded that "[w]hile the Internet has not reached the status where a temporary posting on a newsgroup is akin to publication in a major newspaper or on a television network, those with an interest in using the Church's trade secrets to compete with the Church are likely to look to the ["alt.religion.scientology"] newsgroup [where the documents were posted]. Thus, posting works to the Internet makes them 'generally known' to the relevant people . . ." *Id.* Judge Whyte noted, however, that:

> The court is troubled by the notion that any Internet user, including those using 'anonymous remailers' to protect their identity, can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. . . . [O]ne of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers . . . can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation. . . . Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.

Id. (citations and footnotes omitted).

4. In *Ford Motor Co. v. Lane,* 67 F. Supp. 2d 745 (E.D. Mich. 1999), a court in Michigan refused to enjoin the publisher of blueoval.com from releasing plaintiff's trade secrets on his website. The court concluded that Ford's requested preliminary injunction would have amounted to a prior restraint. In point of fact, there was some

suggestion in the facts of the case that the publisher was acting in collusion with an employee bound by a confidentiality agreement such that the publication would have been equivalent to a misappropriation. Other courts might have ruled differently on the same facts.

D. Trade Secrets Transmitted By Email

A former vice president of Borland Int'l and the C.E.O. of Symantec Corp., a direct competitor of Borland, were indicted by a Santa Cruz County, California grand jury for criminal theft of trade secrets based in part on email messages that Eugene Wang, the former Borland executive, allegedly sent to Gordon Eubanks, Symantec's C.E.O., on the day Wang resigned his position at Borland to go to work for Symantec. *People v. Eubanks,* 47 Cal. App. 4th 158, 48 Cal. Rptr. 2d 778 (1995), *vacated,* 14 Cal. 4th 580, 59 Cal. Rptr. 2d 200 (1996). The charges against the defendants ultimately were dismissed.

E. Commercially Marketed Software

Software may constitute or incorporate trade secrets. *E.g., MAI Systems Corp. v. Peak Computer, Inc.,* 991 F.2d 511, 522 (9th Cir. 1993), *cert. dismissed,* 510 U.S. 1033 (1994); *Data General Corp. v. Grumman Systems Support Corp.,* 36 F.3d 1147, 1165 (1st Cir. 1994); *Gates Rubber Co. v. Bando Chemical Industries, Ltd.,* 9 F.3d 823, 849 (10th Cir. 1993). Even commercially marketed software, when in source code form, may be deemed to constitute or incorporate a trade secret. *E.g., Vermont Microsystems, Inc. v. Autodesk, Inc.,* 88 F.3d 142, 147-51 (2d Cir. 1996).

F. The Inevitable Disclosure Doctrine

The inevitable disclosure doctrine is a judicial doctrine generally associated with a 1995 Seventh Circuit decision, ***PepsiCo, Inc. v. Redmond.*** 54 F.3d 1262 (7th Cir. 1995). Where recognized, the doctrine may provide authority under state trade secret law for restraining a former employee from assuming responsibilities for a competitor comparable to those which she previously held, where the nature of her new position is such that, regardless of her intent, she would inevitably (or even inadvertently) use, rely upon or disclose trade secrets belonging to her former employer, in performing her new duties. Alternatively, where a court is not inclined to prevent an employee from working for a competitor, the risk of inevitable disclosure may justify an order screening out the employee from working on specific technologies or business plans. In Internet-related litigation, the doctrine is increasingly cited by companies with new technologies or market plans as a basis for protecting the value of lead-time when an employee knowledgeable about time-sensitive trade secrets departs to work for a competitor.

1. **Legal Basis.** The inevitable disclosure doctrine arose out of section 2 of the Uniform Trade Secrets Act which authorizes injunctive relief in cases involving "actual or *threatened* misappropriations." The doctrine has served as the basis for injunctive relief in cases where a former employee had signed a noncompetition agreement, although the existence of such an agreement is by no means required. *See, e.g., Branson Ultrasonics Corp. v. Stratman,* 921 F. Supp 909 (D. Conn. 1996); *Ackerman v. Kimball Int'l,* 652 N.E.2d 507 (Ind. 1995); *La Calhene Inc. v. Spolyar,* 938 F. Supp. 523 (W.D. Wisc. 1996). Since restrictive covenants may be independently enforceable under state contract law, the doctrine more commonly is invoked where a defendant did not sign a noncompete contract and relief is premised on the enforcement of a confidentiality agreement. *See, e.g., PepsiCo, Inc. v. Redmond,* 54 F.3d 1262 (7th Cir. 1995); *Southwestern Energy Co. v. Eickenhorst,* 955 F. Supp. 1078 (W.D. Ark. 1997); *Merck & Co. v. Lyon,* 941 F. Supp. 1443 (M.D.N.C. 1996); *Doubleclick, Inc. v. Henderson,* Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997); *see generally* Ian C. Ballon, "The Internet Applications of the Inevitable Disclosure Doctrine," The Cyberspace Lawyer, Feb. 1998.

2. **State by State Review.** A number of courts have declined to apply the inevitable disclosure doctrine in individual cases, but none has expressly rejected it. *See, e.g., Campbell Soup Co. v. Giles,* 47 F.3d 467 (1st Cir. 1995) (Massachusetts law); *APAC Teleservices, Inc. v. McRae,* 985 F. Supp. 852 (N.D. Iowa 1997); *Bridgestone/Firestone, Inc. v. Lockhart,* 5 F. Supp. 2d 667 (S.D. Ind. 1997); *Glaxo Inc. v. Novopharm Ltd.,* 931 F. Supp. 1280 (E.D.N.C. 1996), *aff'd on other grounds,* 110 F.3d 1562 (Fed. Cir. 1997). Injunctive relief under, or consistent with, the inevitable disclosure doctrine has been entered by courts pursuant to section 2 of the UTSA in Arkansas, Delaware, Illinois, Indiana, Iowa, North Carolina and Wisconsin, and in one state, New York, which has not adopted the UTSA. *See Southwestern Energy Co. v. Eickenhorst,* 955 F. Supp. 1078 (W.D. Ark. 1997); *American Totalisator Co. v. Autotote Ltd.,* Civil Action No. 7268, 1983 Del. Ch. LEXIS 401 (Del. Ch. Aug. 18, 1983); *PepsiCo Inc. v. Quaker Oats Co.,* 54 F.3d 1262 (7th Cir. 1995) (Illinois); *Ackerman v. Kimball Int'l,* 652 N.E.2d 507 (Ind. 1995); *Uncle B's Bakery v. O'Rourke,* 920 F. Supp. 1405, 1435, *modified,* 938 F. Supp. 1450 (N.D. Iowa 1996); *Lumex, Inc. v. Highsmith,* 919 F. Supp. 624 (E.D.N.Y. 1996); *Doubleclick, Inc. v. Henderson,* Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997); *Merck & Co. v. Lyon,* 941 F. Supp. 1443 (M.D.N.C. 1996); *LaCalhene Inc. v. Spolyar,* 938 F. Supp. 523 (W.D. Wisc. 1996). Since the UTSA has been adopted by forty states, the inevitable disclosure doctrine is likely to continue to gain favor. *See* Ian C. Ballon, "The Internet Applications of the Inevitable Disclosure Doctrine," The Cyberspace Lawyer, Feb. 1998. For an analysis of the applicability of the inevitable disclosure doctrine under California law, which generally prohibits enforcement of noncompetition agreements, *see* Ian C. Ballon, "Inevitable Disclosure Under California Law," *Intellectual Properties,* Feb. 1998.

3. In ***Doubleclick, Inc. v. Henderson,*** Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997), an Internet advertising firm obtained a preliminary injunction prohibiting two former Doubleclick executives from competing with their ex-employer for a period of six months. The court found that Doubleclick was likely to prevail on claims of breach of the defendants' duty of loyalty, misappropriation of trade secrets and unfair competition based on evidence that the two defendants had openly planned to form a competing Internet advertising agency while still employed by Doubleclick, which undoubtedly colored the court's assessment of the inevitability of defendant's use or disclosure of trade secrets. Important to the court's ruling was its finding that the Internet advertising business is "an extremely competitive one, with a variety of companies using different software and sales techniques to maximize the effectiveness of its clients' advertising." In this context, defendants' work for their own competing agency would have, in the court's view, inevitably resulted in their use of Doubleclick trade secrets because, given their importance to Doubleclick's operations, the court found it "unlikely that they could 'eradicate [Doubleclick's] secrets from [their] mind.'"

4. **Internet Applications of the Doctrine.** The inevitable disclosure doctrine may be especially important to Internet businesses given the speed with which both web-based technology and business models have been developing, the value of lead-time to the development of both Internet technologies and business models and, in the context of technology-based trade secrets, the possibility that a given new technology may be primarily or exclusively associated with a single employer. Where applicable, the inevitable disclosure doctrine may provide a remedy where an employee's technical knowledge of his former employer's trade secrets, know-how or technology is so highly specialized, or where the technology is so closely associated with a single inventor or company, that it would be impossible for the employee to work in the same field without inevitably using, relying upon or disclosing his former employer's proprietary secrets.

Next Section / **Contents**

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

VI. SOFTWARE PATENTS

A. Overview

Unlike copyright and trade secret protection, which generally may be claimed for most original software programs, patent protection is available only for programs that meet the more rigorous requirements of the patent statute (e.g., novelty, utility, nonobviousness). There is often a trade-off between seeking patent protection for a program, and treating it as a trade secret, since the patentable elements of the program must be disclosed in order to obtain a patent (and, in many foreign countries, must be disclosed at the time an application is filed). The law governing patent protection for computer software is somewhat confused. What is apparent, however, is that it has become easier to obtain software-related patents in light of recent Federal Circuit decisions. In addition, new PTO guidelines for patent examiners, adopted in early 1996, are specifically intended to facilitate the issuance of more software patents. *See* U.S. Patent & Trademark Office, Examination Guidelines for Computer-related Inventions (Feb. 1996).

B. What is Patentable?

1. Patent protection is available for the invention or discovery of "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof . . ." 35 U.S.C. § 101.

a. An invention must be a machine, manufacture, composition of matter or a process, or an improvement to any of these four categories, in order to qualify for patent protection. *E.g., In re.*

b. The Supreme Court has held that Congress intended that patents be granted for "anything under the sun that is made by man." *Id. quoting Diamond v. Chakrabarty,* 447 U.S. 303, 309 (1980), quoting S. Rep. No. 1979, 82nd Cong., 2d Sess. 5 (1952); H.R. Rep. No. 1923, 82nd Cong., 2d Sess. 6 (1952).

2. A program that merely makes insubstantial improvements over prior art will not be entitled to patent protection. Specifically, a "patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains." 35 U.S.C. § 103.

C. Computer Software and Internet Business Models

1. The Supreme Court has held that patent protection is *not* available for "laws of nature, natural phenomena, and abstract ideas." *Diamond v. Diehr,* 450 U.S. 175, 185 (1981).

2. Mathematical algorithms have been held to be per se unpatentable. *See Diamond v. Diehr,* 450 U.S. 175, 185 (1981); *Gottschalk v. Benson,* 409 U.S. 63, 75 (1972). The rationale for this rule, however, has not been clearly stated. In Diehr the Court viewed mathematical algorithms as part of the laws of nature, while in *Benson* the Court treated them as ideas. *In re Alappat,* 33 F.3d 1526, 1543 n.19 (Fed. Cir. 1994).

3. In the past, courts applied a two-step protocol known as the Freeman-Walter-Abele test, the first step of which was to determine whether a mathematical algorithm was recited directly or indirectly in the claim and the second step of which was to determine whether the claimed invention as a whole is no more than the algorithm itself. *E.g., In Re Schrader,* 22 F.3d 290, 292 & n.5 (Fed. Cir. 1994).

4. The Federal Circuit limited the Freeman-Walter-Abele test in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.,* 149 F.3d 1368 (Fed. Cir. 1998) to purely mathematical applications. The court wrote that a claim containing a mathematical formula meets the requirements for patentability when the formula "implements or applies that formula in a structure or process which, when considered as a whole, is performing a function which the patent laws were designed to protect (e.g., transforming or reducing an article to a different state or thing) . . . ." According to the Federal Circuit, "[t]he dispositive inquiry is whether the claim as a whole is directed to statutory subject matter. It is irrelevant that a claim may contain, as part of the whole, subject matter which would not be patentable by itself." *Id.* at 1375. The test for patentability focuses on its practical utility.

5. *State Street Bank & Trust Co.* also stands for the proposition that methods for conducting business online are potentially patentable. In that case, the Federal Circuit held patentable a data processing system that allowed an administrator to monitor and record financial information flows (including daily asset allocations, income, expenses and related information) and allowed for several mutual funds to pool their resources. A number of e-commerce patents have issued since the late 1990s.

D. Patent Protection Can Be Lost Through Premature Disclosure

1. U.S. patent protection may be lost if:

a. The invention was known or used by others in the United States, or patented or described in a printed publication anywhere in the world, before the applicant's claimed date of invention; or

b. The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the patent application; or

c. The applicant has abandoned the invention; or

d. The invention was first patented by the applicant in a foreign country more than 12 months before the date of the U.S. application; or

e. The invention was described in an earlier patent; or

f. The applicant was not the actual inventor; or

g. Before the date of the applicant's invention, the invention was made in the United States by someone else who has not abandoned, suppressed or concealed it.

35 U.S.C. § 102.

2. The requirements for obtaining foreign patents may be even stricter than in the United States, and in many countries an invention must be disclosed at the time the application is filed, which can, under certain circumstances, jeopardize U.S. rights.

E. Internet Patent Litigation

E-data Corp. (formerly known as Interactive Give Express, Inc.) has brought two lawsuits to enforce a patent which it contends encompasses all electronic transactions that involve the transfer of digital information. E-data Corp.'s patent, which it acquired in 1995 and which issued in 1985, recites a system and method for selling and distributing digitized products, including video games, movies, software, books, greeting cards, sheet music, audio recordings and other information, and was written in the early 1980s to allow record store customers to create their own customized recordings from a database of digitized songs. James Evans, "E-data's Patent is Alarming Defendants," S.F. Daily Journal, June 10, 1996.

1. ***Interactive Gift Express, Inc. v. CompuServe, Inc.,*** Case No. 95-CV-6871 (S.D.N.Y). Interactive Gift Express, Inc. filed suit in August 1995 against 21 software companies, including Adobe Systems, Inc., and CompuServe, Inc., alleging that it holds patent rights for selling software to individuals over the Internet. Plaintiff alleges that the defendant-software distributors are infringing its patent for "reproducing information in material objects at a point-of-sale location." For the opinion construing Freeny's patent claims, *see* 47 U.S.P.Q.2d 1797 (S.D.N.Y. 1998).

2. ***E-data Corp. v. Micropatent Corp.,*** Case No. 96-CV-523 (D. Conn.). E-data Corp. filed suit in March 1996 against 22 other companies for patent infringement. Some companies, including IBM and VocalTec Ltd., previously purchased licenses to avoid or settle litigation. Edupage, Apr. 4, 1996, *citing* Investor's Business Daily, Apr. 4, 1996, at A8.

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

VII. LICENSES AND ANTITRUST CONSTRAINTS

A. Software and Information

1. **The First Sale Doctrine.** Software vendors typically license, rather than sell software, since a licensor can restrict a licensee's use of software under a license while, under the "First Sale Doctrine," the right to restrict subsequent use (subject to certain exceptions) is lost once the product is sold. See 17 U.S.C. § 109(a). To the extent a "license" is really a disguised sales agreement, however, its restrictive provisions will be deemed unenforceable.

2. **Shrink wrap and click-through licenses.**

a. Consumer software licenses are analyzed under the U.C.C. and traditional contract principles. *See Ohio v. Perry,* 83 Ohio St. 3d 41, 697 N.E.2d 624 (1998) (quoting an earlier version of this paper); *see also Hill v. Gateway 2000, Inc.,* 105 F.3d 1147 (7th Cir. 1997); *ProCD, Inc. v. Zeidenberg,* 86 F.3d 1447 (7th Cir. 1996); *Step-Saver Data Systems, Inc. v. Wyse Technology,* 939 F.2d 91 (3d Cir. 1991); *Arizona Retail Systems, Inc. v. The Software Link, Inc.,* 831 F. Supp. 759 (D. Ariz. 1993). Today, many consumers obtain software preloaded onto personal computers, or packaged in boxes at retail stores, where the terms of a license are buried in documentation. As software increasingly is marketed over the Internet, the enforceability of consumer license agreements should continue to improve because consumers will be expressly asked to accept the terms of a license as a precondition of their being granted access to software. *See* Ian C. Ballon, "Tearing Shrinkwrap in Cyberspace," The Cyberspace Lawyer, Aug. 1996, at 2; *see also Hotmail Corp. v. Van Money Pie, Inc.,* 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998) (assuming - without analyzing - the enforceability of a click-through agreement).

b. **Unconscionability.** In ***Brower v. Gateway 2000, Inc.,*** 246 A.D.2d 246, 676 N.Y.S.2d 569 (N.Y. Sup. Ct. 1998), an intermediate appellate court in New York held the very same form contract at issue in Hill v. Gateway 2000, Inc. unenforceable because unconscionable. The court generally approved of the "cash now, terms later" form of unilateral contract used by Gateway 2000, but ruled that the arbitration clause contained in the agreement was unconscionable under UCC § 2-302 because of the excessive cost associated with I.C.C. arbitration, which the court characterized as "unreasonable" and wrote "surely serves to deter the individual consumer from invoking the process . . . . " The court concluded that the cost of ICC arbitration was prohibitive, particularly given the amount of the typical consumer claim involved.

> For example, a claim of less than $50,000 required advance fees of $4,000 (more than the cost of most Gateway products), of which the $2,000 registration fee was nonrefundable even if the consumer prevailed at the arbitration. Consumers would also incur travel expenses disproportionate to the damages sought . . .
>
> c. **UCITA and the UETA.** In July 1999 the National Conference of Commissioners of Uniform State Laws (NCCUSL) approved the Uniform Computer Information Transactions Act (UCITA; formerly known as proposed UCC Article 2B), which is intended to govern software and information contracts, and the Uniform Electronic Transactions Act (UETA), which is intended to provide a parallel structure for other forms of electronic contracts. UCITA and the UETA are intended to replace paper-based concepts like *writings* with the more modern term *records*. Similarly, records are to be *authenticated,* rather than signed under the new proposed model laws. Copies of the model laws may be obtained at **http://www.law.unpenn.edu/bll/ulc/ucita/** and **http://www.law.unpenn.edu/bll/ulc/fnact99/1990s/uetast84.htm**.
>
> As of this writing, Maryland and Virginia had adopted UCITA and a number of states had enacted the UETA.

3. **Infringement by exceeding the scope of a license.** In a true license, a licensor grants a licensee fewer rights than it is granted under patent or copyright law. A licensee who exceeds the scope of its license can be held liable for patent or copyright infringement. *E.g., S.O.S., Inc. v. Payday, Inc.,* 886 F.2d 1081, 1087?89 (9th Cir. 1989).

4. **Breach of contract.** A licensee who violates the terms of a license also may be sued for breach of contract. As the scope of copyright protection for computer software has narrowed, contract rights may prove increasingly valuable.

5. **Website Terms and Conditions.** Although website Terms and Conditions may constitute enforceable contracts when formatted as click-through contracts, in *Ticketmaster Corp. v. Tickets.com, Inc.,* CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000), the court declined to enforce posted Terms and Conditions that users were not required to review. Posted T&Cs, however, may be found enforceable under UCITA and in other contexts.

B. Music Available Over the Internet

1. **In General.** The way in which music may be used on a site - and in particular whether merely a composition or a particular pre-existing recording will be used - will determine which type of licenses may be required. To reproduce a pre-existing recorded song over the Internet, licenses must be obtained for both the underlying musical composition and the particular recording used. Permission from the songwriter (or assignee) and/or her publishing company to perform the work typically are obtained from BMI, ASCAP or SEAC, while reproduction or distribution rights usually may be obtained from publishers through the Harry Fox Agency.

2. **Webcasting.** Webcasting is the act of transmitting audio or video over the Internet (which currently relies on streaming technology) for simultaneous viewing. Many radio and television stations may be accessed live over the Internet using streaming media players. Other streaming audio or video files are simply stored on a website where they may be viewed or heard at any time.

The Digital Millennium Copyright Act (DMCA) creates a new compulsory license for certain Internet-specific music transmissions (and non-exempt simulcasts) whose primary objective is not to "sell, advertise, or promote particular products other than sound recordings, live concerts, or other music-related events," subject to specific limitations on the number of works from the same phonorecord or artist that may be played in a set time period and the requirement that (other than an announcement immediately preceding a recording) advance programming schedules not be made available. To be eligible for the compulsory license, a website owner also must comply with a number of other specific requirements. 17 U.S.C. § 114(d); Robert W. Clarida, "New Rules for Webcasters," Intellectual Property Strategist, Dec. 1998, at 7. Otherwise, a website owner must negotiate a specific license from the rights owner.

3. **Downloadable Music/ MP3 Files.** MP3 (an abbreviation for the MPEG-1 Audio Layer 3 audio compression algorithm) files are highly compressed CD-quality digital audio files that may be downloaded in a reasonable amount of time for later use. In contrast to analog music recordings, digital files may be quickly and easily downloaded and copied (including for unauthorized purposes) without any material degradation in sound quality from the original.

a. **Litigation.** In October 1998, the Recording Industry Association of America (RIAA) filed suit to prevent Diamond Multimedia Systems from manufacturing or marketing the Rio media player, which is a small, portable device that allows MP3 files to be played. The RIAA alleged that the Rio player did not meet the requirements for digital audio recording devices under the Audio Home Recording Act of 1992 (17 U.S.C. §§ 1001 *et seq.*) because it did not employ a Serial Copyright Management System (SCMS) that sends, receives, and acts upon information about the generation and copyright status of the files it plays. See id. § 1002(a)(2). In affirming the District Court's denial of a preliminary injunction, the Ninth Circuit ruled that the Rio did not qualify as a "digital audio device" within the meaning of the statute because it did not reproduce, either "directly" or "from a transmission," a "digital music recording." *Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc.,* 180 F.3d 1072 (9th Cir. 1999).

b. **SDMI.** The Recording Industry Association of America (RIAA) is promoting the proposed Secure Digital Music Initiative (SDMI), which would restrict the number of times a digital audio file could be reproduced. The development of industry-standard anti-piracy technology will facilitate the widespread availability of MP3 files.

c. **DMCA anti-piracy provisions.** Provisions of the Digital Millennium Copyright Act prohibiting circumvention of "a technological measure that effectively controls access" to a protected work, which are set to take effect on October 28, 2000 (*See* 17 U.S.C. § 1201), and related prohibitions on the sale or distribution of anti-circumvention tools or services which already are in effect, should increase music industry confidence in their ability to curb piracy (although even prior to October 28, 2000, disabling an anti-piracy device could subject a person to liability for contributory copyright infringement).

The DMCA prohibits the manufacture, importation, provision, offer to the public or trafficking in "any technology, product, service, device, component, or part thereof" that

- "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a protected work;
- "has only limited commercially significant purpose or use other than" circumvention; or
- which is marketed for purposes of circumvention.

See id. § 1201(a)(2). A technological measure "effectively controls access to a work" if, in the ordinary course of its operation, it "requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to the work." *Id.* § 1201(a)(3)(B). Circumvention of a technological measure, in turn, is defined to mean "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without authority of the copyright owner . . . ." *Id.* § 1201(a)(3)(A). Similar restrictions are imposed on efforts to restrict the protections afforded by a technological measure. *See id.* § 1201(b).

These anti-circumvention provisions are not intended to alter the standards for third party copyright liability or impose specific design obligations on consumer electronics, telecommunications or computer manufacturers. *See id.* § 1201(c). Exceptions also are created for nonprofit libraries, archives and educational institutions, for law enforcement, intelligence and other government activities and for certain reverse engineering and encryption research. *See id.* §§ 1201(d), 1201(e), 1201(f). For a critique of the provisions governing reverse engineering, *see* Jonathan Band & Taro Issihiki, "The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step," The Cyberspace Lawyer, Feb. 1999, at 2.

4. **Case Law.** A number of lawsuits have been brought against companies such as MP3.com and Napster that facilitate copying of both authorized and infringing music files.

a. In ***RealNetworks, Inc. v. Streambox, Inc.,*** No. C 99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000), the court granted in part and denied in part plaintiff's application for a preliminary injunction. RealNetworks, Inc. had alleged that the defendant's distribution and marketing of "Streambox VCR" and Ripper programs - which could be used to bypass anti-circumvention aspects of RealNetworks' streaming files - violated section 1201 of the DMCA. Streambox VCR allowed users to access and download copies of RealMedia files that otherwise are intended to be streamed over the Internet - but not downloaded. The Streambox Ripper, by contrast, was a file conversion application that allowed RealMedia files to be converted to other formats such as .wav, .rma and MP3. The program also permitted conversion between each of these formats. The court enjoined defendant's distribution of Streambox VCR, but declined to enjoin Ripper, which it found had legitimate purposes and commercially significant uses. In so ruling, the court concluded that the fair use defense under the Copyright Act had no application to claims under section 1201. The court also held that unlike under the Copyright Act, a copyright owner was not automatically entitled to a presumption of irreparable injury under section 1201.

b. In ***Universal City Studios, Inc. v. Reimerdes,*** 82 F. Supp. 2d 211 (S.D.N.Y. 2000), the court preliminarily enjoined distribution of DeCSS - a software utility intended to allow users to break the Content Scramble System (CSS), which is an encryption-based security and authentication system that requires the use of appropriately configured hardware (such as a DVD player or computer DVD drive) to decrypt, unscramble and playback (but not copy) motion pictures stored on DVD. In so ruling, the court ruled that the DMCA did not violate the defendants' First Amendment rights.

c. In ***UMG Recordings, Inc. v. MP3.com, Inc.,*** 92 F. Supp. 2d 349 (S.D.N.Y. 2000), the court entered partial summary judgment in favor of the plaintiffs, ruling that MP3's practice of copying music files to a database to facilitate user copying (in connection with its my.mp3.com service) constituted a violation of the Copyright Act. MP3 had taken a number of precautions designed to ensure that only owners of legitimate copies of protected CR ROMs could make copies of the music files stored on its database. Among other things, it required users to certify that they owned a genuine copy, insert a genuine copy in their computer disk drive or purchase a copy from a cooperating online retainer. MP3 had argued that this practice allowed users to make personal copies of songs permitted under *Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417 (1984); *see generally supra* § II(E). The court, however, found that MP3.com's acts of copying (as opposed to end user copying) did not amount to a fair use. The case ultimately settled with MP3.com agreeing to pay royalties to certain settling record companies.

d. In ***A&M Records, Inc. v. Napster, Inc.,*** No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243 (N.D. Cal. May 5, 2000), Judge Marilyn Patel ruled that Napster was not entitled to benefit from the DMCA liability limitations (*supra* § II(G)) otherwise available to "service providers."

C. Limitation on Licenses: Intellectual Property Misuse

1. **Copyright misuse.** A copyright owner may not prevail in an infringement action if there is an "attempted use of a copyright to violate antitrust laws" or if a "copyright is being used in manner violative of the public policy embodied in the grant of a copyright." *Lasercomb America, Inc. v. Reynolds,* 911 F.2d 970-78 (4th Cir. 1990); *see also Practice Management Information Corp. v. American Medical Association,* 121 F.3d 516 (9th Cir. 1997); *DSC Communications Corp. v. DGI Technologies,* 81 F.3d 597, 601 (5th Cir. 1996) (following Lasercomb). Most other courts that have considered the copyright misuse doctrine since 1990 have declined to apply it.

2. **Patent misuse.** The doctrine of patent misuse, by contrast, has long been established in patent law. *E.g., United States Gypsum Co. v. National Gypsum Co.,* 352 U.S. 457, 465 (1957). Patent misuse may be predicated on actual, or merely proposed license terms. *See, e.g., Motorola, Inc. v. Kimball Int'l, Inc.,* 601 F. Supp. 62, 65 (N.D. Ill. 1984).

3. **Trademark and domain name misuse.** In *Juno Online Services, L.P. v. Juno Lighting, Inc.,* 979 F. Supp. 684 (N.D. Ill. 1997), a court rejected the theory of trademark misuse in a domain name dispute.

4. *Trade secrets licenses*. To avoid copyright or patent misuse problems, especially in view of the lower level of copyright protection now afforded computer software,

software licenses frequently encompass trade secrets as well as other intellectual property rights in software. A software program may be protectable as a trade secret even where copyright or patent protection is unavailable. *E.g., Gates Rubber Co. v. Bando Chemical Industries, Ltd.,* 9 F.3d 823 (10th Cir. 1993).

D. The 1995 U.S. Department of Justice Antitrust Guidelines limit certain licensing practices.

E. Microsoft settlement. In 1994, the U.S. Department of Justice reached agreement with Microsoft on the terms of a consent decree, by the terms of which Microsoft agreed to curb certain software licensing practices, including the practice of charging hardware manufacturers a per-machine royalty (regardless of whether Microsoft's operating system was preloaded onto a given PC). Initially, the district court declined to approve the consent decree. *United States v. Microsoft Corp.,* 159 F.R.D. 318 (D.D.C.), *rev'd,* 56 F.3d 1448 (D.C. Cir. 1995). Among other concerns, Judge Sporkin found that the decree did not address Microsoft's alleged practice of using "Vaporware" (preannouncing software before it exists) to freeze out competitors. The Court of Appeals reversed Judge Sporkin, and, on remand, District Court Judge Thomas Penfield Jackson approved the consent decree. Michelle Quinn, "Judge OKs Pact Settling Microsoft Antitrust Case," The San Francisco Chronicle, Aug. 22, 1995, at A-1.

F. Internet-related Antitrust Litigation

1. ***United States v. Microsoft,*** 147 F.3d 935 (D.C. Cir. 1998).

The D.C. Circuit reversed the District Court's entry of a preliminary injunction prohibiting Microsoft from requiring computer manufacturers who license its Windows operating system to also license and preinstall Microsoft's browser program, Internet Explorer, finding that the government had failed to show a reasonable probability of success on the merits. The suit, originally filed by the Department of Justice in 1997 and subsequently joined by the Attorneys General of 20 states and the District of Columbia, sought to hold Microsoft in contempt for violating the consent decree settling earlier antitrust litigation. In view of the procedural posture of the case - a contempt application to enforce an earlier consent judgment - the outcome turned in large part on contract construction and was affected by the higher burden of proof imposed on a party seeking a contempt sanction than otherwise would have arisen if the Justice Department had simply filed a new action.

a. **Majority Opinion.** In the majority opinion written by Judge Stephen Williams, the D.C. Circuit found that the lower court had failed to provide adequate notice before entering injunctive relief, had misconstrued the meaning of the relevant provision of the consent decree and had appointed a special master without justification. Between the lines, the majority expressed significant skepticism of the government's allegations of an illegal tie-in between Windows 95 and Internet Explorer, although it did acknowledge that Microsoft's operating system dominance created "an exceptional risk of monopoly."

b. **Increasing Returns to Scale and Network Externalities.** Perhaps most influential will be the D.C. Circuit's analysis of the unique nature of the software industry, which it wrote was characterized by increasing returns to scale and network externalities.

(1) **Increasing returns to scale.** According to Judge Williams, "because most of the costs of software lie in the design, marginal production costs are negligible.

Production of additional units appears likely to lower average costs indefinitely." Stated more dramatically, Judge Williams wrote that "the average cost curve never turns upward."

(2) **Network Externalities.** Network externalities may be explained by the fact that "an increase in the number of users of a particular item of software increases the number of other people with whom any user can share work." As a result, "Microsoft's large installed base increases the incentive for independent software vendors to write compatible applications and thereby increases the value of its operating system to consumers."

(3) **Limited Guidance.** Given the limited nature of its ruling and the record on appeal, Judge Williams did not offer substantial guidance on how antitrust law should respond to these factors.

c. **Judge Wald's Concurrence.** Judge Wald, concurring in part and dissenting in part, agreed that the case should be remanded for further consideration but strongly disagreed with the level of deference that the majority concluded should be paid to Microsoft's assertions about its technology, which she characterized as coming close to endorsing "judicial abdication in the face of complexity." Judge Wald instead would have applied a balancing test - evaluating whether the integration of different software products yielded real benefit to consumers (or what she called synergies) and evidence that a genuine market existed for the two products when provided separately.

2. ***United States v. Microsoft,*** 2000 U.S. Dist. LEXIS 8721 (D.D.C. June 7, 2000). Following a trial on the merits, the District Court recommended the break-up of Microsoft.

3. ***Intergraph Corp. v. Intel Corp,*** 195 F.3d 1346 (Fed. Cir. 1999). The Federal Circuit reversed Judge Edwin B. Nelson's entry of a mandatory preliminary injunction which, although phrased in negative terms, essentially compelled Intel Corp. to continue to cooperate with Intergraph Corp. and provide it with information on new products. Intel, the world's largest designer, manufacturer and supplier of high-performance microprocessors (which in 1996 earned 88% of all revenue from microprocessors sold for use in desktop computers, laptops, servers and workstations), was sued by Intergraph, Corp., a workstation manufacturer that abandoned its own proprietary chips in favor of Intel's in the early 1990s, when Intel used an open architecture. Integraph alleged that thereafter, once Intel shifted to treating its chips as proprietary, Intel refused to sell its products to Intergraph. Intergraph alleged that it was "locked in" to Intel's chips, which (together with advance sales and information, which Intel previously had provided to Intergraph and continued to supply to other OEMs) constituted an essential facility.

4. ***Kesmai Corp. v. America Online, Inc.*** (E.D. Va. Complaint filed Sept. 29, 1997).

a. ***Claims.*** Kesmai Corp., leader in the field of aggregate online massively multiplayer computer games - or video games available online that are intended to be played by thousands of people simultaneously - brought suit against AOL for Sherman Act 2 violations (monopolization, attempt to monopolize, monopoly leveraging), false designation of origin and misappropriation, false advertising,

trademark dilution, fraud, breach of contract, defamation, tortious interference with prospective business relations, tortious interference with prospective economic advantage and injunctive relief to block AOL's proposed acquisition of CompuServe under Section 7 of the Clayton Act, 15 U.S.C. § 18. Plaintiff alleged that the online interactive game industry was projected to earn $130 million in 1997, $100 million of which would be generated through AOL. AOL filed a counterclaim in March 1998 alleging malicious prosecution.

b. **Allegations.** AOL, the plaintiff alleged, launched its game channel in 1995. Kensai, which entered into an agreement with AOL to provide content on this channel, initially became one of AOL's top content providers accounting for 25% of total game channel usage. In August 1996, however, AOL purchased INN, a multiplayer game aggregator and developer alleged by Kesmai to have inferior technology that prevented AOL from even carrying it on its game channel until June 1997. After AOL changed its rate structure to a flat fee monthly rate of $19.95, Kesmai alleges that AOL threatened and pressured it to enter into a new agreement on less favorable terms, and provided assurances that Kesmai would be provided the same terms and promotional opportunities as INN. Kesmai alleged that AOL pressured it to allow AOL to purchase it and, when Kesmai refused, AOL placed INN - an AOL subsidiary and Kemsai's direct competitor -in charge of managing AOL's relationship with Kesmai, despite its promise not to do so. AOL also allegedly made INN the exclusive "anchor tenant" for its game channel, after first offering to allow Kesmai to be an anchor tenant as well for between $5-$10 million (which plaintiff alleged was a monopoly rent demanded for the privilege of reaching AOL's 8 million subscribers). Kesmai further alleged that AOL converted all active Kesmai games, which previously could be accessed free of charge, into surcharged premium games, while falsely advising customers that Kesmai, not AOL, was responsible for the change. Kesmai also alleged that two weeks after inducing Kesmai to enter into a new agreement, AOL announced that INN's name was being changed to WorldPlay - which would also be the new name for AOL's game channel - and set up a games menu that effectively rebranded plaintiff's games and created the false impression that plaintiff's games were marketed by WorldPlay. AOL also allegedly denied it any further promotions.

As a consequence of the alleged acts, Kesmai alleged a 92% decrease in usage and related injuries from false statements attributing the new pricing structure to Kesmai and a resulting deterioration of its relations with game developers. Kesmai alleged that AOL also sought to fix prices. Plaintiff alleged that AOL had monopoly power because it was not possible to get enough participants at web-based game sites to make the market for massively multiplayer computer games viable on the web. Plaintiff also noted, as evidence of its monopoly power, even though AOL lost 200,000 customers when it experienced substantial traffic problems after it introduced its flat rate pricing plan, more than half of these customers returned after concluding there was no viable alternative to AOL. Plaintiff defined the relevant markets by product (for the entire country): (1) the sale of online content and Internet access service to customers; (2) the aggregation of online interactive multiplayer games; and (3) the purchase of aggregated games content by online services.

c. **Settlement.** The case ultimately settled on the eve of trial when court papers that had been kept under seal would otherwise have been publicly disclosed *See* Dan Godin, "AOL Gaming Fight Goes to Court," C/NET, June 16, 1998, **http://www.news.com/News/Item/0,4,23229,00.html?st.ne.ni.rel** .

The settlement provided for the parties to continue to work together through at least February 2001 and allowed Kesmai to continue as a significant aggregator of games for the AOL games channel. Other terms of the settlement were not publicly disclosed. Reuters, "Kesmai and AOL Settle Dispute," July 6, 1998.

5. ***Cyber Promotions, Inc. v. America Online, Inc.,*** 948 F. Supp. 456 (E.D. Pa. 1996). In a November 1996 decision, junk email company Cyber Promotions was found not likely to prevail on the merits of its claim that AOL monopolized or attempted to monopolize the market for providing advertising material via electronic transmissions to AOL subscribers. Judge Weiner rejected Cyber Promotions' arguments that the ability to advertise to AOL's subscribers over the Internet via email was an "essential facility" and that AOL has "refused to deal" with Cyber Promotions in violation of Section 2 of the Sherman Act. The court declined to adopt Cyber Promotions' definition of the relevant market as "the market for providing direct marketing advertising material via electronic transmission to AOL's subscribers" because Cyber Promotions and AOL are not direct competitors and antitrust law does not forbid a private company such as AOL "from excluding from its system advertisers like Cyber [Promotions] who refuse to pay AOL any fee (as opposed to those advertisers who do pay a fee) for their advertising on AOL's system." *Id.* at 462, *citing Monsanto Co. v. Spray?Rite Service Corp.,* 465 U.S. 752, 761 (1984). The court noted that AOL was not blocking Cyber Promotions' email messages in order to charge anticompetitive prices, but was merely doing so because Cyber Promotions was bombarding AOL servers with up to 1.9 million advertisements per day without paying for them. The court found that there were numerous competitive methods for advertisers such as Cyber Promotions to reach AOL subscribers, including over the Internet. Finally, the court wrote that AOL had legitimate business justifications for blocking Cyber Promotions' email including that it had received the numerous complaints from its subscribers and was burdened by millions of email advertisements sent to its servers and the fact that Cyber Promotions refused to pay AOL any fee to carry its email advertisements.

6. ***GTE New Media Services, Inc. v. Ameritech Corp,*** Civil Action No. 97-CV-2314 (D.D.C. complaint filed Oct. 1997). GTE filed suit in federal court in Washington, D.C. against Netscape Communications, Yahoo! Inc. and five regional Bell telephone companies on October 6, 1997 alleging a conspiracy to limit competition in the emerging market for online yellow page directories. GTE contends that the Bell entities pooled resources to be carried exclusively on Netscape's home page, whose reference section is maintained by Yahoo! Inc.

Next Section / Contents


The 2nd Annual Spring Meeting


BUSINESS LAW SECTION

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

VIII. TORT LIABILITY OF ONLINE SERVICE PROVIDERS

The scope of tort liability for online content providers was defined in a series of First Amendment cases arising primarily in New York state and federal courts, and in 1996 was modified by Congress.

A. **No Liability Where an Online Service Acts Like a Book Store, Newsstand or Television Network**

1. ***Cubby, Inc. v. CompuServe Inc.,*** 776 F. Supp. 135 (S.D.N.Y. 1991).

a. **Facts:** CompuServe was sued for libel, defamation and unfair competition under New York state law based on allegedly libelous statements about plaintiff's database, Skuttlebut, which were posted on Rumorville USA, a publication available on the Journalism Forum of CompuServe. Rumorville was published by Don Fitzpatrick Associates ("DFA"), which had no employment, contractual or other direct relationship with CompuServe. DFA provided Rumorville to the Journalism Forum under a contract with CCI, an independent company that contracted with CompuServe to "manage, review, create, delete, edit and otherwise control the contents of" the Journalism Forum "in accordance with editorial and technical standards and conventions of style as established by CompuServe." The Journalism Forum's contract with DFA obligated DFA to accept total responsibility for the contents of Rumorville. CompuServe had no opportunity to review Rumorville USA's contents before it was uploaded, and received no part of any fees charged users for access to Rumorville. CompuServe subscribers pay flat monthly and time usage fees, regardless of the information services they use.

b. **Holding:** Summary judgment was entered in CompuServe's favor on all claims. The court held that CompuServe, as the equivalent of "an electronic, for profit library," was entitled to the same First Amendment protection as a news vendor (and therefore would be subject to liability for infringement only if it knew or had reason to know of the allegedly defamatory statements), rather than a publisher, subject to a lower standard of proof. The court wrote that "CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so." *Id.* at 140.

c. **Vicarious liability.** The court rejected plaintiff's contention that CCI or DFA could be considered agents of CompuServe since each of the

three entities were independent of one another. The court characterized CompuServe's right under its contract with CCI to remove text from its system for noncompliance with its standards as merely a means of maintaining "control over the results of CCI's independent work." Id. at 143. Similarly, the court determined that contractual provisions calling for CompuServe to provide CCI with training, necessary support and to indemnify CCI from claims resulting from information appearing in the Journalism Forum did not give CompuServe sufficient control over CCI and its management to render CCI an agent of CompuServe. The court further rejected the notion that CompuServe could be vicariously liable for the actions of DFA, since DFA's contract was with CCI.

2. ***Stern v. Delphi Internet Services Corp.,*** 165 Misc. 2d 21, 626 N.Y.S.2d 694 (N.Y. Sup. Ct. 1995).

a. **Facts:** Controversial radio talk show celebrity Howard Stern brought suit against Delphi Internet Services Corp. for commercial misappropriation of his name and likeness based on Delphi's use of a picture of Mr. Stern exposing his buttocks to promote an online bulletin board service, which Delphi had set up for subscribers to debate the merits of Mr. Stern's candidacy for governor of New York.

b. **Analogy to a television network.** The court held that the "incidental use" exception, which is grounded in the First Amendment interest in protecting the ability of news disseminators to publicize their own communications, shielded the defendant from liability. The court analyzed the similarities between an online service and a news vendor or book store, or a letters-to-the-editor column of a newspaper, ultimately concluding that Delphi Internet Services Corp. was analogous to a television network in its dissemination of both news and entertainment.

B. *Stratton Oakmont v. Prodigy Services, Inc.*: Liability Where Systems Operator Exercises Some Degree Of Editorial Control.

Stratton Oakmont v. Prodigy Services, Inc., Index No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (Nassau County, N.Y. Sup. Ct. May 26, 1995):

1. **Facts.** An anonymous Prodigy subscriber posted allegedly defamatory messages about the brokerage firm Stratton Oakmont and its president on "Money Talk," a widely read financial bulletin board where members can post statements regarding stocks, investments and other financial matters. Stratton Oakmont and its president sued Prodigy for defamation, seeking $200 million in damages.

2. **Prodigy was held to be a "publisher"** (and therefore subject to liability for defamation regardless of actual or imputed knowledge).

3. ***Cubby*** **distinguished.** The court found that:

a. Prodigy held itself out as a family-oriented online service that exercised editorial control over the content of messages on its bulletin boards, thereby expressly differentiating itself from its competitors and likening itself to a newspaper.

b. Prodigy in fact regulated the content on its bulletin boards by (a) promulgating "content guidelines," (b) using software that

automatically prescreened all bulletin board postings for offensive language, and (c) using "Board Leaders" to enforce Prodigy's content guidelines.

c. In *Cubby*, CompuServe had no opportunity to review the contents of the publication at issue before it was uploaded.

4. **"Board Leader" an agent of Prodigy.** The court held that for the limited purpose of monitoring and editing "Money Talk," the Board Leader was an agent of Prodigy, notwithstanding express language to the contrary in Prodigy's Bulletin Board Leader Agreement, because Board Leaders were required to follow procedures established by Prodigy, which exercised managerial control over the Leaders.

5. **Policy implications**. Will this decision discourage online services from policing the conduct of their subscribers? Is this decision inconsistent with copyright law cases on contributory infringement which penalize sysops who take a laissez-faire attitude about materials posted on their BBSs (*supra* § II(F))? Do the holdings of *Cubby* and *Stratton Oakmont* suggest that online services should hire third parties to police their subscribers' conduct and relinquish important control functions to these unrelated entities? How practical are these solutions?

6. **Appeal.** Prodigy filed a notice of appeal. "Cameo Clips," Entertainment Law & Finance, July 1995, at 2.

7. Settlement/motion for reargument denied.

a. **Settlement.** In October 1995, a provisional settlement was reached. Stratton Oakmont agreed to support Prodigy's assertion that it is not a publisher and is not liable for the acts of anonymous subscribers. Michelle Quinn, "Online Libel Suit Dropped," The San Francisco Chronicle, Oct. 25, 1995, at B1.

b. **December 1995 Opinion.** On December 13, 1995, Judge Ain *denied* Prodigy's motion to vacate the court's May 26, 1995 opinion even though Stratton Oakmont supported Prodigy's motion, and the parties' settlement was conditioned on the court vacating its prior decision. Judge Ain reasoned that litigants would be discouraged from settling cases early in litigation if they knew that courts would, as a matter of course, vacate unfavorable rulings when requested to do so as a condition of settlement. In addition, Judge Ain wrote that his prior opinion dealt with

> a developing area of law [that] has thus far not kept pace with the technology . . . [creating] a real need for some precedents. To simply vacate that precedent on request because these two parties (or this plaintiff) has lost interest or decided that the litigation would be costly or time consuming would remove the only existing New York precedent in this area leaving the law even further behind the technology.

C. The Telecommunications Act of 1996

1. ***Stratton Oakmont* overruled.** Section 509 of the Act provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230 (c)(1). Congress intended the provision to overrule *Stratton Oakmont*

v. Prodigy Services, Inc. and any similar decisions that have treated online "providers and users as publishers and speakers of content that is not their own because they have restricted access to objectionable material." Conference Report 104-458, 104th Cong. 2d Sess. 194 (1996). The Act expressly preempts inconsistent state laws, but does not prevent states from enforcing laws consistent with the purpose of the Section. 47 U.S.C. § 230(e)(3).

2. **Policy objectives.** The purpose of this portion of the Telecommunications Act is to promote the development of the Internet and other interactive computer services and media, preserve the free market for the Internet and online services without state or federal government regulation, encourage the development of technologies that maximize user control over what information is received, remove disincentives for the development and use of blocking and filtering technologies that parents may use to restrict children's access to objectionable or inappropriate online material and ensure the enforcement of federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer. 47 U.S.C. § 230(b).

3. **Effect of the law.** Section 230 does not completely insulate online services from liability for defamation. By reversing *Stratton-Oakmont,* subpart (1) codifies a modified version of the *Cubby* standard under which a service provider (or user) may be held indirectly liable for third party acts of defamation only in instances where it actually knew that material posted online was defamatory and failed to take any action, or in very limited circumstances where it failed to act despite reason to know that material was defamatory (provided that the basis for imputed knowledge is not the provider's acts of monitoring online content). *See* Ian C. Ballon, "*Zeran v. AOL*: Why the Fourth Circuit Is Wrong," Journal of Internet Law, Mar. 1998, at 6. While subpart (1) essentially codifies *Cubby,* subpart (2) (as discussed below (*infra* § VIII(D)(2)) immunizes providers who take certain good faith measures consistent with the Act - such as screening online content - from liability based on that conduct, thus also eliminating liability based on imputed knowledge in certain circumstances. *See* Ian C. Ballon, "Defamation and Preemption Under the Telecommunications Act of 1996: Why the Rule of *Zeran v. America Online, Inc.* Is Wrong," The Cyberspace Lawyer, July/Aug. 1997, at 6. *But see Zeran v. America Online, Inc.,* 129 F.3d 327 (4th Cir. 1997) (holding that section 230 eliminates both republication and distributor liability), *cert. denied,* 524 U.S. 937 (1998).

D. The Scope of Preemption of State Claims

1. ***Zeran v. America Online, Inc.***, 129 F.3d 327 (4th Cir. 1997), *cert. denied,* 524 U.S. 937 (1998).

a. **Facts.** A pseudonymous AOL subscriber posted plaintiff's name and home phone number on purported advertisements for highly offensive and vulgar t-shirts celebrating the bombing of the Oklahoma City federal building and praising accused bomber Timothy McVeigh. Zeran learned of the posting on April 25, 1995 (the day it appeared) when a reporter called him. Zeran immediately notified AOL, which assured him that the notice would be removed (although AOL, consistent with its stated policy, refused to post a retraction). Zeran was inundated with angry phone calls. Although the notice was deleted by AOL the day after it was posted, on April 26, 1995, a new notice appeared later that same day. Zeran again contacted AOL, which advised him that the new message would be deleted and that AOL was taking steps to terminate the account of the pseudonymous subscriber known only as "Ken ZZ03." Nonetheless, similarly offensive messages continued to be posted through May 1, 1995. To make matters worse, a DJ in Oklahoma City received a copy of the bogus

posting, read it on the air, and urged his listeners to call "Ken." Zeran claimed to have received hostile and offensive telephone calls as a result of the posting at the rate of about once every two minutes in late April 1995. Plaintiff, at AOL's suggestion, contacted the FBI, and was placed under protective surveillance by local police. The deluge of threatening calls continued until May 15, 1995, when they subsided to about 15 per day.

b. **Zeran's Suit.** In April 1996, after the Telecommunications Act was signed into law, Zeran filed suit against AOL for negligence.

c. **Holding.** The court held that Zeran's claim was preempted because the Telecommunications Act of 1996 preempts state law and immunizes online providers (and others) from liability not only for republication of defamatory statements (as in *Stratton Oakmont*) but also for distribution of defamatory material. Whether AOL knew or should have known that "Ken ZZ03"'s defamatory statements were posted online therefore was irrelevant. In the *Zeran* court's view, the Telecommunications Act of 1996 overruled both *Stratton Oakmont* and the rule of law set forth in *Cubby.*

d. **Criticism.** For a critique of the *Zeran* decision, *see* Ian C. Ballon, "*Zeran v. OAL:* Why the Fourth Circuit Is Wrong," Journal of Internet Law, Mar. 1998, at 6; Ian C. Ballon, "Defamation and Preemption Under the Telecommunications Act of 1996: Why the Rule of Zeran v. America Online, Inc. Is Wrong," The Cyberspace Lawyer, July/Aug. 1997, at 6.

e. **Post-*Zeran* case law.** Two courts have uncritically applied *Zeran. See Blumenthal v. Drudge,* 992 F. Supp. 44 (D.D.C. 1998); *Doe v. America Online, Inc.,* 718 So. 2d 385 (Fla. App. 1998). In a less controversial application, the court in *Jane Doe One v. Oliver,* 46 Conn. Supp. 406 (Conn. 2000), ruled that section 230 preempted negligence and other state law claims.

2. **Broad preemption of state claims and remedies.** The Good Samaritan exemption contains two separate subparts. 47 U.S.C. § 230(c)(1) provides absolute immunity from republication liability for any provider or user covered by the Act, while Section 230(c)(2) provides broad immunity in any cause of action where liability is sought to be imposed "on account of ... any action voluntarily taken in good faith to restrict access to or availability of material . . . considered to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ." Specifically, the Act provides that:

> (1) . . . No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil Liability - No provider or user of an interactive computer service shall be held liable on account of -
>
> > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise

objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

a. **Expansive definition of affected parties.** The term "Information Content Provider" is defined to mean "any person that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3). The definition of "interactive computer service" is broad enough to encompass any computer network, including an employer's computer network or intranet. 47 U.S.C. § 230(f)(2).

b. **Impact.** The Act immunizes network providers or users from a broad range of state law claims where a potential defendant undertook "any action voluntarily . . . in good faith to restrict access to or [the] availability of material that the provider or user considers to be . . . harassing, or otherwise objectionable." Subpart 2 of the Good Samaritan provision also potentially immunizes employers from certain claims based on employee use of email if the employer took steps to come within the scope of the exemption.

3. **Immunity extends to third party (but not original) content.** In *Ben Ezra, Weinstein & Co. v. America Online, Inc.,* 206 F.3d 980 (10th Cir. 2000), the Tenth Circuit affirmed the entry of summary judgment for the defendant in a defamation case based on allegedly inaccurate stock information provided to AOL by third parties. In dicta, the court acknowledged that section 230 immunity would not extend to information that a defendant developed or created itself.

4. **Web host not a content provider**. In *Does v. Franco Productions*, 99 C 7885, 2000 U.S. Dist. LEXIS 8645 (N.D. Ill. June 22, 2000), the court dismissed a suit against a web host pursuant to section 230(c)(2), concluding that plaintiff's claims revolved around third party content (rather than material actually created by the defendants themselves).

E. Bulletin Board Postings Held Not to Be Periodicals

It's In The Cards, Inc. v. Fuschetto, 193 Wis. 2d 429, 535 N.W.2d 11 (1995).

1. **Facts:** Jeff Meneau and It's In The Cards, Inc. brought suit for defamation, negligence and tortious interference with business relations against Rosario Fuschetto, d/b/a Triple Play Collectibles. Fuschetto posted an allegedly defamatory message on a BBS that was accessible to all subscribers of SportsNet, a national computer network.

2. **Holding:** At issue in the case was whether bulletin board postings constituted "periodicals" within the meaning of a Wisconsin statute that provided that a plaintiff had to demand a retraction before bringing a libel action against a "periodical." The court held that "[p]osting a message to the sports bulletin board is a random communication of computerized messages analogous to posting a written notice on a public bulletin board, not a publication that appears at regular intervals."

3. **A plea for legislative action.** The court wrote that "[a]pplying the present libel laws to cyberspace or computer networks entails rewriting statutes that were written to manage physical, printed objects, not computer networks or services. Consequently, it is for the legislature to address the increasingly common phenomenon of libel and defamation on the information superhighway."

F. Tort Liability for Computer Viruses

For a discussion of potential theories, see Vicky H. Robbins, "Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software," 10 Computer Lawyer 20 (1993).

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

IX. EMAIL

A. What Mode of Communication Does Email Replace?

The Florida Supreme Court observed that "email transmissions are quickly becoming a substitute for telephonic and printed communications, as well as a substitute for direct oral communications." *In Re: Amendments to Rule of Judicial Administration, 2.051-Public Access to Judicial Records,* 651 So. 2d 1185 (Fla. 1995). Because email communications take the place of both oral and written communications, can be saved electronically (and therefore potentially accessed by systems operators), printed in hard copy, and easily re-transmitted by recipients, the privacy rights of senders and recipients of email (at least in unencrypted form) are still being defined by courts.

B. When Is Email Private?

1. **Email sent from or received on a home computer via America Online.** In *United States v. Maxwell,* 42 M.J. 568 (U.S. Air Force Crim. App. 1995), *aff'd in relevant part,* 45 M.J. 406 (U.S. Armed Forces Ct. App. Nov. 21, 1996), the U.S. Air Force Court of Criminal Appeals upheld defendant's court martial conviction, but held that the Electronic Communications Privacy Act (18 U.S.C. §§ 25100 *et seq.,*) applies to email transmissions, and found that the defendant had an objective expectation of privacy in email messages stored in AOL's computers which he alone could retrieve through the use of his own assigned password, as well as in email transmitted electronically to other AOL subscribers who had individually assigned passwords. The court wrote that, "unlike transmissions by cordless telephone, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there is virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients. . . . In the modern age of communications, society must recognize that such expectations of privacy are reasonable." On the other hand, the court noted in dicta that the defendant "may well have forfeited his right to privacy to any email transmissions that were downloaded to the computer by another subscriber or removed by a private individual from the on-line service."

A subsequent appellate court concluded that the defendant possessed a "reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL." 45 M.J. at 417. The court noted that "[t]he fact that an unauthorized 'hacker' might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way." *Id.* at 418. The court's finding also rested on the proposition that AOL email is more private than "similar messages on the Internet" because AOL email is privately stored for retrieval on AOL computers and AOL maintains a strict policy of not reading or disclosing subscriber email, which the court considered to be a form of contractual privacy protection. The court wrote - incorrectly - that Internet email is insecure because it passes through

multiple servers. *Id.* at 416. In fact, pursuant to TCP/IP protocols, email transmitted over the Internet is broken into packets which are hard to intercept and, separately, virtually impossible to decipher.

The court also held that email messages posted in a chat room or "'forwarded' from correspondent to correspondent, lose any semblance of privacy." *Id.* at 418. This unqualified determination about the privacy of forwarded messages seems extreme.

2. **Judicial Email.** In *In Re: Amendments to Rule of Judicial Administration, 2.051-Public Access to Judicial Records, 6*51 So. 2d 1185 (Fla. 1995), the Florida Supreme Court analyzed whether email used within the Florida judiciary constituted "official records" which were required to be retained and stored. Recognizing the different modes of communication that email messages can replace, the court determined that official business email transmissions should be treated like other types of official communications received and filed by the judicial branch, while internal email communications, such as those sent by judges to their staffs, would not be subject to public disclosure. In particular, the court cited as examples of the type of email messages that should not be retained as "official records": proposed drafts of opinions and orders, memoranda concerning pending cases, proposed jury instructions, votes on proposed opinions, and information obtained from online research services, such as WestLaw.

3. **U.S. Government and business records.**

a. **U.S. Government Email.** Email sent to or received by government agencies is subject to the Federal Records Act and therefore must be saved in hard copy form. *Armstrong v. Executive Office of the President,* 877 F. Supp. 690 (D.D.C. 1995). Similarly, email messages retained by the Executive Office of the President are "presidential records" subject to the President's Records Act. *See American Historical Association v. Peterson,* 876 F. Supp. 1300 (D.D.C. 1995).

b. **Email may not be a business record.**

(1) One court has held that email does not qualify as a "business record," and therefore is not admissible as an exception to the hearsay rule under Federal Rule of Evidence 803(6), because "email is far less of a systematic business activity than a monthly inventory printout." *Monotype Corp. PLC v. International Typeface Corp.,* 43 F.3d 443, 450 (9th Cir. 1994). The court left open the possibility that email could be admissible for other purposes.

(2) **Express Policy.** A different result might be reached if a company has an express policy governing retention and deletion of email messages.

c. **Employee email is discoverable.** In *Star Publishing Co. v. Burchell,* 181 Ariz. 432, 891 P.2d 899 (1994), the court upheld a lower court order compelling production of employee email communications. The Pima County Board of Supervisors, in connection with allegations concerning improprieties in the operation of the County Assessor's Office, had subpoenaed the computer backup tapes of the Assessor's Office containing all documents for 1993, including email communications of employees. While the case appears to have turned primarily on the absence of evidence that the specific email

communications were privileged, the dissenting Judge noted that "this may indeed be a case where technology has once again outpaced the law."

C. Encryption and Internet Security

1. **Encryption.**

a. Encryption is the process of converting data (stored in digital form as a series of 1s and Os) into an incomprehensible code through use of an algorithm. Encryption increases the security of email messages sent over the Internet.

b. One of the most common encryption programs is PGP (an acronym for "Pretty Good Privacy"), which uses the Rivast-Shamir-Adleman (RSA) public/private algorithms to produce encrypted text. RSA algorithms involve complementary pairs of encryption/decryption keys (one key is made public, the other kept private; a document encrypted with one key may be decrypted only with the other key). PGP, however, can only be exported from the United States pursuant to an export license, which must be obtained on a case-by-case basis. Barry D. Bayer & Benjamin H. Cohen, "Keeping Electronic Messages Secret," The Legal Intelligencer, May 24, 1995, at 8. Bills presently before Congress would ease export restrictions.

c. Encryption is not practical unless a recipient can decrypt an encrypted email message. Since encryption technology cannot be freely exported, encryption programs are of limited value in international communications. Until encryption programs are widely used, interoperable and internationally available, it is not practice to expect that most Internet email communications will be encrypted.

2. **Litigation over encryption export controls.**

a. ***Karn v. Department of State,*** 925 F. Supp. 1 (D.D.C. 1996).

(1) **Facts.** Plaintiff submitted commodity jurisdiction requests to the U.S. Department of State to obtain a determination whether he could export the book "Applied Cryptography" by Bruce Schneier and a computer disk containing source code that was reprinted in the book. The State Department determined that the book could be freely exported, but not the disk, which was subject to its jurisdiction under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). Plaintiff argued that the government's designation of the disk, but not the book containing the same source code, as a defense article subject to export controls, was arbitrary and capricious and an abuse of discretion in violation of the Administrative Procedures Act. Karn also argued that defendants' conduct violated his constitutional rights to free speech under the First Amendment and substantive due process under the Fifth Amendment.

(2) **Ruling.** The court dismissed plaintiff's challenge to the State Department's designation of plaintiff's disk as a

"defense article" because the Arms Export Control Act precludes judicial review, and granted summary judgment in favor of the government on defendant's First and Fifth Amendment claims based on the finding that the government's regulations were "content neutral" and the issues raised presented a nonjusticiable political question.

b. A different result was reached in *Bernstein v. Department of State* 974 F. Supp. 1288 (N.D. Cal. 1997), aff'd, 176 F.3d 1132 (9th Cir. 1999). In that case, Daniel Bernstein had unsuccessfully attempted to post his Snuffle encryption system and related documentation on an Internet discussion group called "sci.crypt." Bernstein brought suit, alleging that the government's suppression of his program under the AECA and ITAR violated his free speech right to express his scientific ideas by publishing an academic paper on the system (which includes the program's source code). The trial court had granted the defendant's motion for summary judgment ruling that the government's encryption regulations, insofar as they required licenses for encryption and decryption software, devices and technology, constitute unconstitutional prior restraints under the First Amendment.

c. A more recent First Amendment challenge was also decided against the government. *See Junger v. Daley,* 209 F.3d 481 (6th Cir. 2000).

3. **Current Export Regulations.**

a. *1999 ITAR regulations.* Effective April 12, 1999, the government issued new regulations governing export controls of encryption products. The 1999 policy permits export of 56-bit products and their equivalent (including 1024-bit asymmetric systems) to all countries, except Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, after a one-time governmental review. The policy also allows for the export of stronger products to subsidiaries of U.S. entities, health and insurance companies, and certain "electronic commerce" users. It further permits export of encryption products of unlimited strength if the plaintext is "recoverable," (i.e., if the product includes key recovery mechanisms or "backdoor" accesses to the underlying plaintext). *See* 22 C.F.R. §§ 120 to 130.

b. **1998 Financial Institution Export Guidelines.** On July 7, 1998, the Secretary of Commerce announced new export guidelines that applied only to financial service encryption products. *See* Encryption Items, 63 Fed. Reg. 50516 (1998). Under the revised policy, financial institutions in 45 countries may apply for a one-time license to use encryption of any strength in the United States without the requirement for built-in key-recovery systems. The revised policy was applauded in public comments as a necessary step for global financial commerce over the Internet, but was criticized because it did not apply to other types of organizations.

4. **Other security measures.**

a. **Digital signatures.**

(1) The Internet presently operates on the NFS (Network File System) protocol, which does not allow users to

determine whether files or messages have been altered during transmission. Digital signatures use cryptographic techniques to identify the author of a work and verify that the contents of a file have not been altered. A digital signature contains a unique sequence of digits computed based on the work being protected, the particular algorithm being used and the key used in generating the signature. A work containing a digital signature may or may not be encrypted. NII White Paper at 187; Wall Street Journal, Oct. 11, 1995, at B6.

(2) For a copy of the 1996 Digital Signature Guidelines prepared by the Information Security Committee of the ABA's Section of Science and Technology, contact the Section at (312) 988-5599 or sciencetech@attmail.com.

b. **Steganography**. Also known as "digital fingerprinting" or "digital watermarking." Digital information may be encoded with attributes that cannot be disassociated from the file that contains the information. NII White Paper at 188.

D. Email, Client Confidences and the Attorney-Client Privilege

1. **Reasonable protection.**

Canon 4 of the ABA's Model Code of Professional Responsibility obligates attorneys to "preserve the confidences and secrets" of their clients. Reasonable measures, but not absolute security is what is required. Ronald Abramson, "Protecting Privilege in E-mail Systems," Texas Lawyer, Sept. 5, 1994, at 20.

2. **Is the use of email reasonable?**

a. Interception is unlawful. The interception by unintended recipients of email messages transmitted over public communication lines is unlawful under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et seq.; *United States v. Maxwell,* 42 M.J. 568 (U.S. Air Force Crim. App. 1995), *aff'd in part,* 45 M.J. 406 (U.S. Armed Forces Ct. App. Nov. 21, 1996); *see also People v. Stevens,* 34 Cal. App. 4th 56, 63, 40 Cal. Rptr. 2d 92, 96 (1995) (summarizing the ECPA's legislative history).

b. **Internet security.**

(1) It is virtually impossible to intercept an email while in transit over the Internet. Pursuant to TCP/IP protocols, information is transmitted over the Internet in packets. A single message may be broken into several different packets, which may be sent over different routes before being reassembled at their destination point. A single packet would be almost impossible to target and virtually unintelligible.

(2) Many of the concerns about the security of email apply to other modern forms of communications. For example, it is easier to tap a telephone line than intercept an email while in transit. Similarly, many lawyers have received misdirected confidential faxes, yet still routinely

transmit confidential documents by facsimile.

c. **Gateway security**. The connection point between a company or law firm's internal network and the Internet must be protected by a firewall to prevent intruders from hacking into a computer network.

d. **Internal security employed by lawyers and clients.** The reasonableness of a lawyer's use of email for attorney-client communications should depend in large measure on the policies for use, retention and destruction of email implemented by both the law firm and the client. While no one set of procedures is likely to be determinative, companies should adopt policies to ensure that attorney-client communications are treated confidentially. Among issues to consider are: who routinely has access to email? is access determined by a password? could anyone in the company retrieve the message? are confidential communications routinely transmitted outside of the control group?

e. **Is encryption required?** Given how difficult it is to intercept an email in transit it should generally be viewed as unnecessary to encrypt email communications, although the additional security will provide protection in case a message is misaddressed. If a communication is encrypted while in transit, decrypted and then left in an email box on an unsecured network, forwarded outside of the control group or otherwise inadequately protected, the fact that it was encrypted while in transit will have little effect on whether it remains confidential. Internal use of encryption - or adequate policies - may be more important than encrypting messages sent over the Internet.

3. **Case law.**

a. **Disclosure destroys privilege.** Once arguably privileged communications are made available over the Internet, they are in the public domain and any claim to privilege may be lost. *See Castano v. The American Tobacco Co.,* 896 F. Supp. 590, 595-96 (E.D. La. 1995) (tobacco industry documents widely disseminated over the Internet; applying California rules of conduct).

b. **Inhouse communications.** At least one lower court has expressly ruled that inhouse email communications may be protected. In *National Employment Insurance Corp. v. Liberty Mutual Ins. Co.,* No. 93-2528-G (Mass. Sup. Ct. Dec. 21, 1994), a Massachusetts state court judge ruled that email messages sent between a corporation's inhouse counsel and middle and low-level employees were privileged because undertaken for legal, rather than business purposes. In the alternative, Judge Welch ruled that the email messages were immune from discovery as attorney-work product. "Current Developments" in The Computer Lawyer, Jan. 1995, at 29.

4. **Ethics Opinions.**

In early 1999, the ABA Standing Committee on Ethics and Professional Responsibility issued Opinion No. 99-413, which provides that it is generally reasonable for attorneys to communicate with clients by email.

Several states previously had issued ethical opinions warning against using email for attorney-client communications. These early decisions appear to have been

made without an appreciation of the difference between the way information is sent over the Internet and the manner by which it is transmitted to analog cellular phones. Increasingly, states are issuing ethical opinions recognizing that it is generally appropriate to communicate with clients by unencrypted email. *See, e.g.*, Illinois Ethics Op. 96-10 (May 16, 1997); North Dakota Op. 97-09 (Sept. 1997); South Carolina Ethics Op. 97-08 (June 1997); Vermont Opinion 97-5; *see also* Iowa Ethics Op. 97-01 (Sept. 18, 1997) (communications acceptable with written waiver); *see generally* **http://www.legalethics.com**.

E. An Employer's Right to Monitor Employee Email.

Employees typically send and receive personal email messages in much the same way that they may place and receive personal telephone calls while at work. However, unlike telephone calls (unless recorded, which generally is prohibited absent a court order), email communications are stored electronically (unless and until deleted by the recipient) and can be monitored, either intentionally by employers or surreptitiously by co-workers.

1. In ***Bohach v. Reno, 9***32 F. Supp. 1232 (D. Nev. 1996), Judge Edward Reed denied plaintiff's application for a preliminary injunction based on alleged violations arising out of the Reno police department's monitoring alphanumeric pager messages which the plaintiffs, who were both police officers, sent each other over the department's "Alphapage" message system. The system was actually a software program that allowed brief alphanumeric messages to be transmitted to visual display pagers. The software was installed in mid-1994, at which time police officers were told that "every Alphapage message is logged on the network" and should not be used for certain types of messages (such as comments about Department policy or remarks that would violate the Department's anti-discrimination policy). Messages were typed on computers, where they were stored on a server even after transmitted via modem to a paging company for transmission by radio broadcast. The Department's computers could be freely accessed; a password or special clearance was not required. The initial phase of this process, according to the court, "is essentially electronic mail - and e-mail messages are, by definition, stored on a routing computer." *Id*. at 1234. The court held that the officers did not have an objectively reasonable expectation of privacy in these communications and therefore were not likely to prevail on their Fourth Amendment civil rights claim.

2. ***Smith v. Pillsbury Co.,*** 914 F. Supp. 97 (E.D. Pa. 1996). A federal district court in Philadelphia, applying Pennsylvania state law, held that an employee who was fired for the contents of an email he transmitted from a company computer, had no cause of action for wrongful termination. The court found that the employee did not have a reasonable expectation of privacy in his email messages, even though the company had assured its employees that their private email communications would be treated confidentially and would not be intercepted, because the plaintiff sent an offending message over the company's email system to his supervisor. Even if the employee had a reasonable expectation of privacy, the court reasoned that a company's need to deter unprofessional and potentially illegal conduct outweighs any countervailing privacy interest, especially since the court determined that a company's interception of employee email is not highly intrusive.

3. California state trial courts that have considered the issue have upheld an employer's right to monitor employee email. Ricardo Sandoval, "E-mail is Next Frontier in Privacy Debate," San Jose Mercury News, Aug. 13, 1995, at E-1; Abdon M. Pallasch, "Company Policies to Monitor E-mail Licking Edge of Electronic Envelope," Chicago Lawyer, Aug. 1995, at 4. For an alternative view of the privacy issues surrounding employee email, *see* Larry O. Gantt, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," 8 Harv. J.L. & Tech. 346 (1995).

F. Liability for Email Transmissions

1. **Employer liability of employee email.** While an employer may, under certain circumstances, be held liable for employee email, it may also be able to claim immunity under the Good Samaritan provisions of the Telecommunications Act of 1996 if it took some action to regulate its computer network. Specifically, an employer who actively undertakes to monitor email as part of "any action voluntarily taken in good faith to restrict access to or [the] availability of material that the provider or user considers to be . . . harassing, or otherwise objectionable" may immunize itself from certain torts and other state law claims based on employee use of a company's email system or intranet. 47 U.S.C. § 230(c)(2); *see supra* § VIII(D).

2. **Employee email as evidence of a crime.** A former vice president of Borland Int'l and the C.E.O. of Symantec Corp., a direct competitor of Borland, were indicted by a Santa Cruz County, California grand jury for criminal theft of trade secrets based in part on email messages that Eugene Wang, the former Borland executive, allegedly sent to Gordon Eubanks, Symantec's C.E.O., on the day Wang resigned his position at Borland to go to work for Symantec. People v. Eubanks, 38 Cal. App. 4th 114, 44 Cal. Rptr. 2d 846 (1995), vacated, 96 C.D.O.S. 9329 (Cal. Dec. 23, 1996). The Santa Cruz County District Attorney dismissed charges against Eubanks in November 1996, while the case was pending before the California Supreme Court.

G. Challenging Email Anonymity Under the ECPA

Privacy laws generally compel service providers to maintain the confidentiality of subscriber information. The identity of a pseudonymous actor, however, may be obtained from Service Providers by subpoena pursuant to the Electronic Communications Privacy Act (ECPA). *See Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105 (E.D. Mich. 1998) (dismissing or entering judgment for the defendant on plaintiff's alleged privacy, breach of contract and tort claims (among others) arising out of AOL's disclosure of plaintiff's identity pursuant to a facially valid subpoena in accordance with the provisions of the Electronic Communications Privacy Act).

H. Spoliation of Evidence

Companies should adopt adequate email, intranet, extranet and electronic communication policies in order to avoid liability for spoliation of email evidence in the event of litigation. *See* Ian C. Ballon, "Spoliation of E-mail Evidence: Proposed Intranet Policies and A Framework For Analysis" *The Cyberspace Lawyer,* Mar. 1999; Ian C. Ballon, "How Companies Can Reduce The Costs and Risks Associated With Electronic Discovery," *The Computer Lawyer,* July 1998.

Next Section / **Contents**

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

X. SPAMMING AND THE LAW OF JUNK EMAIL

A. Definition

Spamming, or the practice of disseminating multiple unsolicited copies of junk email over the Internet, is considered a violation of netiquette, and has been the subject of several notable lawsuits. Some companies that distribute mass email advertisements use pseudonymous - or false - return email addresses (and phony headers), so that their identity cannot be traced. By masking the true source of a junk email transmission, spammers increase the likelihood that the message will be opened and read, rather than automatically deleted by recipients. Spammers also avoid being burdened by complaints and email bombs that are routinely sent by recipients by return message.

By using false return email addresses, commercial bulk email distributors impose costs and burdens on the Internet providers whose domain names they use. First, misaddressed emails, which ordinarily are automatically returned to sender, are routed to the false return address used by the spammer. Since the user id typically does not exist, rather than being returned to a specific email box, the misaddressed email is routed to the postmaster or network supervisor of the server attached to the false return address, who may open the message to try to determine where to reroute it. Second, recipients of junk email often respond by flaming - or sending angry return email messages to - authors of junk email messages; when a false return address is used, these messages, as well, are routed to the network supervisor of the domain name used by the spammer as its false return address.

B. Case Law

1. ***America Online, Inc. v. Cyber Promotions, Inc.*** Cyber Promotions, a company that distributes mass emailings on behalf of its commercial customers, filed suit against America Online, alleging that AOL had tried to put it out of business by sending it "email bombs." America Online responded that it was a violation of AOL's terms and conditions to distribute mass emailings from an AOL account. America Online subsequently filed its own suit against Cyber Promotions, Inc., alleging that Cyber Promotions, Inc. used forged return addresses in its mailings, including *aol.com,* to avoid detection, and that AOL's postmaster workstation was overwhelmed with returned email messages bearing the forged addresses. On April 11, 1996, the parties stipulated to a preliminary injunction barring Cyber Promotions, Inc. from using any of America Online's trademarks, including its aol.com domain name, in junk email communications. *America Online, Inc. v. Cyber Promotions, Inc.*, Civil Action No. C-96-4621 (E.D. Va. 1996).

In a later ruling, granting in part AOL's motion for summary judgment, the court held that Cyber Promotions did not have a First Amendment right to send unsolicited email over the Internet to subscribers of a private network because AOL was not equivalent of a state actor. The court also held that AOL could use blocking software

to prevent its subscribers from receiving email from Cyber Promotions. *Cyber Promotions, Inc. v. America Online, Inc.,* 948 F. Supp. 436 (E.D. Pa. 1996).

The case settled in February 1997. Cyber Promotions dropped its opposition to AOL's use of PreferredMail, which allows subscribers to decide whether to screen out unsolicited email, and agreed to use only one of five domains to send unsolicited email to AOL's subscribers. In the past, Cyber Promotions had used multiple return email addresses to circumvent PreferredMail. Bob Woods, "America Online & Cyber Promotions Split Court Decision," Newsbytes, Feb. 5, 1997.

2. In ***CompuServe Inc. v. Cyber Promotions, Inc.,*** Civil Action No. C2-96-1070 (S.D. Ohio T.R.O. entered Oct. 28, 1996), CompuServe brought suit against Cyber Promotions, Inc. and its president for service mark infringement, unfair competition, deceptive trade practices, conversion or trespass to personal property and nuisance, violation of the Computer Fraud and Abuse Act, misappropriation/unjust enrichment, breach of contract and fraud. CompuServe focused in part on Cyber Promotions false use of headers, which are the legends attached to email messages that show the message's point of origin, route traveled and ultimate destination. The Complaint alleged that "[b]ecause electronic mail provides an opportunity to reach a wide audience quickly and at virtually no cost to the sender, some companies have begun using it to distribute advertisements over the Internet, sending the same unsolicited commercial message to hundreds of thousands of Internet users at once." CompuServe analogized the practice to a telemarketer's calls to a cellular telephone user, because CompuServe subscribers are charged for the amount of time they spend online, and subscribers spend wasted time accessing, reading and deleting junk email messages.

On October 28, 1996, Judge Graham issued a temporary restraining order prohibiting the defendants from falsifying the headers on junk email messages to make it appear as though the messages originated from a CompuServe account (which they did not) on the grounds that such falsification causes undeliverable email messages to be returned to the falsified CompuServe account (as well as angry responses from the recipients of such messages). The TRO also prohibits the defendants from falsely configuring their email to make it appear that the messages originate from CompuServe's domain (which, among other things, allows the messages to circumvent blocking filters that some Internet providers and users employ to avoid receiving junk email).

Judge Graham subsequently issued a preliminary injunction on February 3, 1997, prohibiting Cyber Promotions from sending email messages to CompuServe subscribers, on the theory that Cyber Promotions' failure to adhere to CompuServe's request to cease such transmissions constituted common law trespass. *CompuServe, Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015 (S.D. Ohio 1997).

3. In ***Concentric Network Corp. v. Wallace,*** Case No. C-96-20829-RMW (N.D. Cal. Nov. 13, 1996), Cyber Promotions, Inc. and Sanford Wallace agreed to a broad-reaching injunction prohibiting them from using Concentric Network Corp.'s accounts to send or receive email, misrepresenting that Cyber Promotions' messages were sent from an email address operated by Concentric, sending any unsolicited messages to Concentric subscribers or including Concentric's subscribers on any email list sold to third parties.

4. In ***Hotmail Corp. v. Van Money Pie, Inc.***, 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998), the court held that the plaintiff was likely to prevail on, among other theories, claims based on the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and breach of contract; *see also America Online, Inc. v. LCGM, Inc.,* Civil Action No. 98-102-A,

1998 U.S. Dist. LEXIS 20144 (E.D. Va. partial summary judgment entered Nov. 10, 1998) (granting summary judgment against a spammer in part based on the Computer Fraud and Abuse Act).

5. In ***America Online, Inc. v. Prime Data Systems, Inc.,*** Civil Action No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226 (E.D. Va. Nov. 20, 1998), AOL obtained a default judgment against a group of spammers for violations of the Computer Fraud and Abuse Act, false designation of origin, Virginia common law trespass to chattels, violations of the Virginia Computer Crimes Act and common law conspiracy to commit trespass to chattels and to violate Federal and Virginia statutes. In addition to entering permanent injunctive relief, Magistrate Judge Thomas Rawles Jones, Jr. therefore awarded compensatory damages of $101,400 ($0.00078 x 130,000,000 UBE messages transmitted by defendants and logged by AOL) in addition to awarding attorneys fees under the Lanham Act and punitive damages for trespass to chattels in the amount of $304,200 (treble the amount of compensatory damages). AOL had submitted evidence that it incurred costs of at least $0.00078 per email message sent (exclusive of personnel and other costs tied to the operation of its computers) - or roughly one cent for every 13 messages sent.

C. Administrative Regulation

In ***FTC v. Maher*** (D. Md. Complaint filed Mar. 4, 1998), the FTC brought suit against a spammer for unfair and deceptive marketing practices to consumers.

D. State Regulation

1. **State Statutes.** Several states have enacted laws regulating the dissemination of unsolicited commercial email. *See, e.g.,* Cal. Bus. & Prof. Code §§ 17511.1, 17538.45; Cal. Penal Code § 502.

2. **Litigation.** In *Engst v. World Touch Networks,* No. 98-2-17831-1 (King county, WA Sup. Ct. complaint filed July 17, 1998), a plaintiff brought suit for damages against an alleged spammer under Washington state law.

Next Section / Contents

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

XI. PRIVACY LAWS AFFECTING THE CONDUCT OF ELECTRONIC COMMERCE

A. Overview

Privacy laws affect the conduct of electronic commerce in at least three important respects. First, the practices of website and database owners with respect to their collection, use and dissemination of personally identifiable information - and the disclosures made about these practices - affect consumer confidence in Internet commerce and are the subject of laws (such as the Online Child Protection Act and EU Privacy Directive) and FTC regulation. Second, laws governing privacy potentially affect employee rights in electronic communications (including email) and an employee's use of the Internet or a company's intranet or extranet. See supra § IX. Third, publicity rights (which are a form of privacy right) may be important in licensing website content.

U.S. Data privacy law is comprised of a patchwork of constitutional, statutory and common law privacy rights that afford substantial protection in very narrow areas. Privacy rights are recognized under U.S. law in specific circumstances (such as in the context of criminal investigations or in response to intrusive snooping by strangers), for particular categories of information (such as tax returns, personal financial data or medical records) or for specific classes of people (such as children). By comparison, the protections afforded by U.S. privacy laws are less comprehensive than those mandated by the European Union's Privacy Directive.

U.S. Data privacy law is comprised of a patchwork of constitutional, statutory and common law privacy rights that afford substantial protection in very narrow areas. Privacy rights are recognized under U.S. law in specific circumstances (such as in the context of criminal investigations or in response to intrusive snooping by strangers), for particular categories of information (such as tax returns, personal financial data or medical records) or for specific classes of people (such as children). By comparison, the protections afforded by U.S. privacy laws are less comprehensive than those mandated by the European Union's Privacy Directive.

Increasingly, federal statutes compel particular types of online providers to post specific privacy policies on websites. Such requirements may be imposed in particular on sites that:

- collect information from children (see 15 U.S.C. §§ 6501 to 6506, 16 C.F.R. §§ 312.1 to 312.12)
- constitute "financial institutions" that provide individuals with a financial product or service "primarily for personal, family, or household purposes." (see 15 U.S.C. §§ 6801 et seq.; 16 C.F.R. §§ 313.1 to 313.13); or
- (in the future) handle "individually identifiable health information" (see 42 U.S.C. § 1320d).

B. The EU Privacy Directive

1. **Overview.** The EU Privacy Directive compelled EU member states to adopt uniform rules governing data privacy by October 24, 1998. The Directive treats data

privacy as a fundamental human right and generally protects personal data collected by governments or for business purposes. Data collected for "purely personal" or "household purposes" is outside the scope of the Directive. See Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive No. 95/46/EC (Oct. 24, 1995). A copy may be obtained at **http://www.open.gov.uk/dpr/insnet2.htm**.

2. **Consent or Necessity.** Article 7 provides that personal data generally may only be processed where an individual's consent has been obtained or in certain cases of necessity.

a. **Consent must be "unambiguously given," specific and informed**. A notice buried in website Terms and Conditions will not suffice.

b. **Necessity.** Personal data alternatively may be processed if one of five conditions are met, such as where processing is necessary for the performance of a contract or to protect the vital interests of the data subject.

c. **Free speech.** Article 9 also recognizes an exception for the processing of personal data carried out solely for "journalistic purposes or for the purpose of artistic or literary expression . . . ," but only "if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

d. **Special categories.** Certain categories of data generally may not be processed absent explicit consent (or may not be processed at all, depending on individual national laws implementing the Directive). These categories of data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or disclosing details of a person's health or sex life. *See* Art. 8.

e. **Exemptions.** Member states may exempt data processing from the protections of the Directive where necessary to safeguard: national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offenses; important economic or financial interests of the European Union or a member state; certain inspection and regulatory functions; or the protection of the data subject or the rights and freedoms of others. *See* Art. 13.

3. **Data Quality**. Article 6 compels member states to assure that personal data is processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; accurate, and in certain circumstances kept up to date; and kept in a form which permits identification of individual data subjects only for as long as necessary for the purposes for which the data originally was collected.

4. **Mandatory Disclosures.** Articles 10 and 11 compel controllers to disclose to data subjects their identities; the purpose for which personal data is being processed; and certain additional information such as whether particular information sought must be provided or is merely optional.

5. **The Rights to Access Data and Object to its Processing.** Article 12 provides individuals with limited rights to review and correct personal data. Article 14 further provides limited rights to object to the processing of personal data for direct

marketing purposes or on "compelling legitimate grounds."

6. **Confidentiality and Security.** Data controllers are responsible for ensuring the confidentiality and security of personal data.

7. **Transfer of Personal Data to Third Countries.** Article 25 restricts the transfer of personal data outside of the EU except where third countries ensure "an adequate level of protection . . ." for personal data, as judged by the standards of the Directive. The United States thus far has been found not to provide an adequate level of protection. This poses potential problems for U.S. businesses - especially those with European operations.

C. The U.S. Response to the EU Privacy Directive

1. **Self-regulation.** The FTC has encouraged industry self-regulation. The EU has rejected self-regulation as a basis for meeting the requirements of Article 25.

2. **Technology.** In a June 1998 draft opinion on the Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS), the Working Party of the Commission concluded that a "technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. See European Commission Directorate General XV, Working Party on the Protection of Individuals with regard to the processing of Personal Data, Op. 1/98 (June 16, 1998 Draft).

3. **U.S. Dept. of Commerce Safe Harbor Principles.** In March 2000, the European Union and U.S. Department of Commerce reached agreement on safe harbor principles which, if followed, are intended to allow individual companies a presumption that they provide adequate protections within the meaning of Article 25. *See* **http://www.ita.doc.gov/td/ecom/menu/html**.

D. U.S. Constitution.

1. Privacy rights under the U.S. Constitution include limited rights that protect individuals from government intrusion. The U.S. Supreme Court has recognized an amorphous, albeit limited, constitutional right to privacy in cases involving personal family matters such as contraception and abortion. *See, e.g., Griswold v. Connecticut,* 381 U.S. 479 (1965); *Roe v. Wade,* 410 U.S. 113 (1973).

2. The Fourth Amendment protects individuals' privacy rights against unreasonable searches and seizures and may provide remedies where a person's subjective - yet objectively reasonable - privacy expectations in email have been violated by a government agency acting without a warrant or other permissible grounds for doing so. *See, e.g., Minnesota v. Solson,* 495 U.S. 91, 95 (1990); *United States v. Maxwell,* 45 M.J. 406, 417 (Armed Forces Ct. App. 1996).

E. The California Constitutional Right to Privacy

Article I, section 1 of the California Constitution grants California residents an inalienable right to privacy. Unlike the federal Constitutional right to privacy, the state right is express, rather than implied, and was added in 1972 by Proposition 11, a ballot initiative.

1. **Personal data.** The California right to privacy, which is construed in part based on the arguments advanced in support of the ballot initiative, was directed, among other things, at concerns about entities "gather[ing], keep[ing], and disseminat[ing] sensitive personal information without checking its accuracy or restricting its use to mutually agreed or otherwise legitimate purposes." *Hill v. NCAA,* 7 Cal. 4th 1, 20, 26 Cal. Rptr. 2d 834 (1994). Initiative proponents also argued that Proposition 11 addressed concerns about "collecting and stockpiling unnecessary information"

about individuals, which typically cannot be reviewed and corrected, and "misusing information gathered for one purpose in order to serve other purposes or embarrass" people. Supporters of the initiative specifically cited credit card issuers, insurance companies and employers as entities that collect - and potentially misuse - personal information. Proponents of the initiative also specifically referred to computer-generated data. *Hill v. NCAA,* 7 Cal. 4th at 21-22, *quoting* Ballot Pamphlet, Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) 26-27.

2. **Not Limited to Government Conduct.** Unlike the Fourth Amendment to the federal Constitution, the California right protects California residents in their dealings with both the government and private businesses (including employers).

3. **Private Cause of Action.** Individuals may bring suit to enforce violations of their rights. In order to state a claim for a violation of California's constitutional right to privacy, a plaintiff must show (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that constitutes a "serious invasion of privacy." A defendant may avoid liability "by negating any of the three elements . . . or by pleading and proving, as an affirmative defense, that the invasion of privacy is justified because it substantively furthers one or more countervailing interests." A plaintiff, in turn, may rebut a defendant's assertion of countervailing interests by showing that "there are feasible and effective alternatives to defendant's conduct, which have a lesser impact on privacy interests." *Loder v. City of Glendale,* 14 Cal. 4th 846, 890-91, 59 Cal. Rptr. 2d 696, *cert. denied,* 118 S. Ct. 44 (1997).

F. Common Law

Common law rights of privacy and publicity are based in tort law. Justice Brandeis is generally credited with being the first to articulate a broad theory of a right to privacy in a law review article he authored in 1890. *See* Warren & Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890); Prosser & Keeton, Torts § 117 (5th ed. 1984). The modern law of privacy is traced to William L. Prosser, and an influential law review article he wrote in 1960. Prosser identified four distinct causes of action for invasion of privacy: (1) appropriation of the defendant's name or likeness for commercial benefit; (2) unreasonable intrusion, or intentional interference with a plaintiff's interest in solitude or seclusion (either in his person or in his private affairs); (3) public disclosure of private facts; and (4) publicity which places the plaintiff in a false light. *Zacchini v. Scripps-Howard Broadcasting Co.,* 433 U.S. 562, 571 n.7 (1977), *citing* William L. Prosser, *Privacy,* 48 Calif. L. Rev. 383, 389, 403 (1960).

G. Statutes Protecting Privacy Rights

Federal statutes provide privacy rights for specific categories of information such as video rental records (18 U.S.C. § 2710), cable television subscriber information (47 U.S.C. § 551) and a student's educational records (20 U.S.C. § 1232g). Some of the more important statutes relating to electronic commerce are:

1. **The Fair Credit Reporting Act.** This statute prohibits disclosure of information from a person's credit file (such as credit history or employment data) absent consent. 15 U.S.C. §§ 1681 to 1681u. Non-financial information found in a credit-header (which includes a person's name, aliases, birth date, social security number, current and prior addresses and telephone numbers) is not protected from disclosure by the Act.

2. **The Electronic Funds Transfer Act** requires that contracts with consumers for electronic funds transfers inform consumers when and how information about them may be disclosed. 15 U.S.C. § 1693.

3. **The Child Online Protection Act.** The Child Online Protection Act, passed in late 1998, directs the FTC to adopt regulations by November 1999 requiring operators of commercial websites or online services to (1) provide notice on the website of the type of information it collects from children, how it uses such information and what its disclosure practices are; (2) obtain verifiable parental consent for the collection, use or disclosure of personal information from children; (3) provide certain information to parents, when requested; (4) prohibit conditioning a child's participation in a game or related activity where the child's disclosure of additional personal information "is reasonably necessary to participate in such activity . . . ;" and (5) establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children. The Act will take effect in either April 2000 or April 2001, depending on certain FTC actions taken prior to that time.

4. **The Computer Fraud and Abuse Act** provides civil and criminal remedies when crackers or others break into a computer network (or exceed authorized access) and obtain financial, medical or other information protected by the Act. *See* 18 U.S.C. § 1030.

5. **The Electronic Communications Privacy Act** proscribes the interception of communications while in transit (18 U.S.C. §§ 2510 to 2521) or when stored on a network (18 U.S.C. §§ 2701 to 2711). *See supra* § IX (D).

H. FTC Privacy Guidelines for Fair Information Practices in Consumer Transactions

The FTC, in a June 1998 report to Congress, proposed guidelines for fair information practices in consumer transactions. *See* Privacy Online: A Report to Congress (FTC June 1998). By surveying government studies, both in the United States and other countries, the FTC concluded that it was possible to generalize about core principles of fair information practices. Specifically, the FTC concluded that consumers must be assured:

- Notice of an entity's information practices;
- Choice with respect to how information collected about them is used and disseminated;
- Access to information about them collected and stored by an entity;
- Security that a data collector has taken appropriate steps to ensure the security and integrity of any information collected; and
- Enforcement mechanisms to ensure compliance with these principles, when adopted in practice codes or guidelines.

I. *In re: GeoCities*

The FTC filed a complaint against GeoCities, Inc. alleging that its failure to abide by the terms of its stated privacy policy constituted an unfair or deceptive act or practice within the meaning of section 5(a) of the Federal Trade Commission Act. *In re: GeoCities,* File No. 9823015 (F.T.C. 1998).

GeoCities offers its members free email accounts, free and fee-based personal home pages, contests and children's clubs, among other services. People wishing to obtain free email accounts, personal homepages or other services were required to complete a membership application that included both mandatory and optional information fields. The form also asked applicants to indicate whether they wished to receive "special offers" from advertisers and specific goods or services from individual companies.

1. **FTC Allegations.** First, the FTC alleged that GeoCities falsely represented that the personal identifying information it collected from membership application forms was used only to provide members the specific advertising offers or goods or

services requested. In fact, according to the FTC, GeoCities sold, rented or otherwise disclosed this information to third parties to be used for purposes other than the ones for which permission had been obtained from GeoCities members. Second, the FTC alleged that GeoCities falsely represented that the "optional information" it collected from members was not disclosed to third parties without the member's permission. In fact, the FTC alleged that GeoCities disclosed this information to third parties who used it to conduct targeted advertising to GeoCities members. Third, the FTC alleged that GeoCities falsely represented that it collected and maintained personal identifying information of children who signed up to join the Official GeoCities' GeoKidz Club or to participate in contests. In fact, according to the FTC, such information was collected and maintained by third party "community leaders," who also ran GeoCities' contests.

2. **Consent Judgment.** A consent judgment entered in August 1998 prohibits GeoCities from making any misrepresentation about its collection or use of personal identifying information from or about consumers, including what information will be disclosed to third parties and how the information will be used. GeoCities agree to provide "clear and prominent notice" to consumers of its data collection practices, including at least the following information:

- What information is being collected (e.g., "name," "home address," "e-mail address," "age," "interests");
- Its intended use(s);
- The third parties to whom it will be disclosed (e.g., "advertisers of consumer products," "mailing list companies," "the general public");
- The consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;
- The consumer's ability to remove directly or have the information removed from respondent's databases and the means by which (s)he may do so; and
- The procedures for having personal identifying information deleted from GeoCities' databases and any limitations imposed on such deletion.

The Consent Judgment also contained specific requirements on how GeoCities' new privacy policy would be posted on its website. GeoCities further agreed that it would not collect personally identifying information from any child age 12 or younger if it has actual knowledge that the child does not have the permission of a parent to provide such information. The Judgment further provides that GeoCities shall not be deemed to have actual information where a child has falsely represented the she is an adult and it has no reason to doubt such information.

J. Federal Regulatory Jurisdiction

1. **Opt-in vs. opt-out procedures.** Internet marketers prefer procedures that compel users to affirmatively opt-out of marketing programs. The EU, by contrast, generally requires that consumers be given the choice to opt-in before their data can be used. In different statutes, Congress has adopted both opt-in (in the case of the Driver's Privacy Protection Act) and opt-out provisions (under the Gramm-Leach-Bliley Act).

2. **The Commerce Clause.** In ***Reno v. Condon,*** 120 S. Ct. 666 (2000), the U.S. Supreme Court gave broad approval to the power of Congress to regulate privacy issues pursuant to its authority over interstate commerce. The case concerned the Driver's Privacy Protection Act of 1994 (codified at 18 U.S.C. §§ 2721 to 2725), which prohibits state departments of motor vehicles (DMVs) or their employees or contractors (subject to specific exceptions) from knowingly disclosing or otherwise

making available to any person or entity personal information about any individual obtained in connection with a motor vehicle record. The Court upheld the constitutionality of the Act even though it conflicted with a South Carolina statute that allowed DMV data to be freely marketed to third parties, because the Court concluded that "[t]he motor vehicle information which the States have historically sold is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations" and therefore constituted "an article of commerce," the "sale or release into the interstate stream of business is sufficient to support congressional regulation." In so ruling, Chief Justice Rehnquist, writing for a unanimous Court, rejected South Carolina's Tenth Amendment arguments, because "the DPPA does not require the States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as owners of databases." *Id.* at 671, 672.

3. **First Amendment Limitations.** While Congress undoubtedly could compel use of opt-in procedures pursuant to its power to regulate data in interstate commerce, there is at least some question about whether the FTC could do so in implementing more general federal privacy guidelines. *See U.S. West, Inc. v. FCC,* 182 F.3d 1224 (10th Cir. 1999) (invalidating under the First Amendment an opt-in procedure adopted by the FCC to protect unspecified privacy interests), *cert. denied,* 68 U.S.L.W. 3747 (2000).

Next Section / Contents

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

XII. OBSCENITY AND FREE SPEECH

A. Child Pornography

1. **Distribution and possession illegal.** U.S. law prohibits distribution or possession of child pornography. 18 U.S.C. § 2251; *Osborne v. Ohio,* 495 U.S. 103 (1990).

2. **Reporting Requirement.** Pursuant to the Protection of Children from Sexual Predators Act of 1998 and implementing regulations, anyone engaged in providing an *electronic communication service or a remote computing service* to the public must report "knowledge of facts or circumstances" from which a violation of child pornography laws is apparent to the National Center for Missing and Exploited Children (NCMEC) and the FBI or U.S. Customs Service. Such a report must be made "as soon as reasonably possible" after obtaining knowledge and should include "whatever information . . . that led it to conclude that a violation of federal child pornography statutes" had occurred. The regulations suggest that a report "could include information concerning: visual depictions of child pornography; the identity of persons or screen names or persons transmitting or receiving child pornography; or requests by persons to receive child pornography." *See* 42 U.S.C. § 13032(b); 18 U.S.C. § 2702(b)(6); Proposed Rules of the Department of Justice, 64 Fed. Reg. 28422, 28424 (May 26, 1999). A provider who knowingly and willfully fails to make a required report may be fined up to $100,000 (or $50,000 for an initial violation).

3. **Morphing and virtual child pornography.**

a. Pursuant to the Child Pornography Prevention Act of 1996, it is also now illegal to receive, reproduce or distribute visual images enhanced to appear as though they depict child pornography. 18 U.S.C. § 2252A.

b. **Affirmative Defense.** The Act creates an affirmative defense where the alleged child pornography was created using actual people who were adults at the time the material was produced and "the defendant did not advertise, promote, present, describe, or distribute the material in such a manner as to convey the impression that it is or contains a visual depiction of a minor engaging in sexually explicit conduct." Id. § 2252A(c).

c. **Split in the Circuits.** The constitutionality of the Act has been upheld in at least two circuits. *See United States v. Hilton,* 167 F.3d 61 (1st Cir.), *cert. denied,* 120 S. Ct. 115 (1999); *United States v. Acheson,* 195 F.3d 645 (11th Cir. 1999). *But see The Free Speech*

Coalition v. Reno, 198 F.3d 1083 (9th Cir. 1999).

B. Interstate Transportation of Obscene Material

1. **Transportation and distribution prohibited.** U.S. law prohibits the transportation, distribution or importation of obscene material, which is not protected by the constitutional guarantees of freedom of speech or freedom of press. 18 U.S.C. §§ 1462, 1465; *Roth v. United States,* 354 U.S. 476 (1957). In *Stanley v. Georgia*, 394 U.S. 557 (1969), the U.S. Supreme Court held that individuals have a privacy right to possess obscene materials in their homes. In subsequent decisions, however, the Court has clarified that this right does not create a correlative right to receive, transport or distribute obscene material in interstate commerce.

2. In **United States v. Maxwell,** 45 M.J. 406 (U.S. Armed Forces Ct. App. 1996) the court upheld the court martial conviction of Col. Maxwell for violating federal law by using his personal computer (a) to receive or transport visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252 and (b) to transport in interstate commerce, for the purpose of distribution, visual depictions of an obscene, lewd, lascivious or filthy nature in violation of 18 U.S.C. § 1465. The court reversed the defendant's earlier conviction for using his personal computer to communicate indecent language to another service member via email on his America Online account. The offending conduct occurred on the defendant's home computer during off-duty hours.

3. **United States v. Chapman,** 60 F.3d 894 (1st Cir. 1995). The defendant pled guilty to transporting child pornography in interstate commerce in violation of 18 U.S.C. § 2252(a)(1) for transmitting over America Online to an AOL subscriber in another state three photographs depicting children engaged in sexual acts. In an appeal of his sentence, the First Circuit held that the transmission of child pornography by computer is not "sexual abuse or exploitation" within the meaning of the U.S. sentencing guidelines.

4. **United States v. Thomas,** 74 F.3d 701 (6th Cir. 1996). The defendants were convicted for violating the federal obscenity laws in connection with their operation of a BBS that allowed subscribers to download images and order videotapes by mail of material found to be obscene.

C. The Communications Decency Act: Indecent and Patently Offensive Communications Directed at Minors

In ***Reno v. ACLU,*** 521 U.S. 844 (1997), the U.S. Supreme Court struck down those provisions of the Communications Decency Act ("CDA") which restricted access by interactive computer service to *indecent and patently offensive* communications as an unconstitutional abridgement of free speech. The Court left intact section 223(a) to the extent it applies to "any comment, request, suggestion, proposal, image or other communication which is obscene . . . as opposed to merely indecent."

1. **Vagueness.** The Court found the CDA impermissibly vague, in part because different terminology was used in two parallel sections of the CDA (*indecent* in 47 U.S.C. § 223(a) and material that "in context, depicts or describes, in terms *patently offensive* as measured by contemporary community standards, sexual or excretory activities or organs" in subsection (d)). The Court wrote that it was unclear how these two standards (which were taken from elements of previous Supreme Court tests) related to one-another or just what they meant. For example, although the *patently offensive* language used in the statute was taken from one of the three prongs of the definition for obscene material adopted by the Court in *Miller v. California,* 413 U.S. 15 (1973), the Court wrote that "[j]ust because a definition

including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague."

2. **Breadth.** In ruling that the CDA failed to pass strict scrutiny, the Court emphasized that "[t]he breadth of the CDA's coverage is wholly unprecedented" and therefore "impose[d] an especially heavy burden on the Government to explain why a less restrictive provision would not [have] be[en] as effective as the CDA." The Court noted that the CDA was not limited to commercial speech (and therefore burdened nonprofit organizations and individuals, as well as businesses) and - by virtue of the definitions of *indecent* and *patently offensive* - "cover[ed] large amounts of nonpornographic material with serious educational or other value." The Court further noted that the "community standards" criterion "as applied to the Internet means that any communication available to a nation-wide audience will be judged by the standards of the community most likely to be offended by the message." In addition, the Court also pointed out the absence of congressional findings made it more difficult to conclude that Congress had carefully considered whether less restrictive measures were available.

3. **Justice O'Connor's Zoning Analysis.** Justice O'Connor, joined by Chief Justice Rehnquist, concurred in part and dissented in part, analyzing the CDA as a legitimate attempt "to create 'adult zones' on the Internet." Justice O'Connor found the CDA lacking, however, to the extent that it substantially interfered with the First Amendment rights of adults. She would have invalidated the "display" and "indecency transmission" and "specific person" provisions of the "patently offensive" prong as applied to communications involving more than one adult, but would have upheld the "indecency transmission" and "specific person" provisions insofar as they applied to communications between a single adult and one or more minors.

Justice O'Connor wrote that adult zoning laws have been sustained under the First Amendment if: (1) they do not unduly restrict adult access to the material; and (2) minors have no First Amendment right to read the material.

D. The Child Online Protection Act: Commercial Speech Deemed *Harmful to Minors*

In October 1998, Congress enacted the Child Online Protection Act, 47 U.S.C. § 231 (colloquially referred to as "CDA II" since it reflects an attempt to meet some of the objectives of the Communications Decency Act held unconstitutional in *Reno v. ACLU,* 521 U.S. 844 (1997), while also responding to the specific defects noted by the Supreme Court in that case).

1. **Harmful to minors.** The Act is more narrowly tailored than the CDA and merely regulates the knowing commercial dissemination of content "harmful to minors," when made freely available over the Internet by commercial vendors of adult content. The statute only applies to commercial speech, which is entitled to a lower level of First Amendment protection than other forms of speech, and incorporates the "harmful to minors" or "obscene as to children" standard upheld in the context of magazine vendors in *Ginsberg v. New York,* 390 U.S. 629 (1968).

2. **ISP Exemption.** Among other things, the statute exempts "a person engaged in the business of providing an Internet access service . . . " 47 U.S.C. § 231(b)(2).

3. **Legal Challenge.** The ACLU has filed suit challenging the constitutionality of the law. *See ACLU v. Reno,* 31 F. Supp. 2d 473 (E.D. Pa. 1999) (preliminarily enjoining enforcement of the statute), *aff'd,* Appeal No. 99-1324, 2000 U.S. App. LEXIS 14419 (3d Cir. June 22, 2000).

E. Screening Software

In ***Mainstream Loudoun v. Loudoun County Library,*** 24 F. Supp. 2d 552 (E.D. Va. 1998), Judge Leonie Brinkema granted summary judgment in favor of the plaintiffs, finding that a public library's use of screening software violated the First Amendment. She wrote that while the library was "under no obligation to provide Internet access to its patrons," once it decided to do so the First Amendment restricted its ability to limit patrons' access.

F. State Regulation of the Internet

1. ***American Library Association v. Pataki,*** 969 F. Supp. 160 (S.D.N.Y. 1997). In a ruling issued just days before the U.S. Supreme Court struck down most of the CDA in *Reno v. ACLU,* a lower court in New York entered a preliminary injunction barring enforcement of N.Y. Penal Law § 235.21(3) which, like the CDA, prohibited certain forms of inappropriate communications directed at minors. The court's decision, however, turned on the Commerce Clause, rather than the First Amendment. The court found that, because geographic boundaries do not exist in cyberspace, the statute represented an unconstitutional projection of New York law into conduct that occurs wholly outside of the state. In addition, the court concluded that the burdens imposed by the law on interstate commerce outweighed any local benefit derived from it. Finally, and perhaps most dramatically, the court concluded that the Internet "requires a cohesive national scheme of regulation . . . " and that "[t]he need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the Commerce Clause."

2. ***ACLU v. Miller,*** 977 F. Supp. 1228 (N.D. Ga. 1997). A federal court in Atlanta entered a preliminary injunction barring enforcement of a Georgia statute which made it a crime for any person to knowingly transmit data over a computer network using a false identification or knowingly using a third party's trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely state or imply that such person had permission or was legally authorized to do so. In a decision rendered just days before the U.S. Supreme Court issued its opinion in *Reno v. ACLU,* the court found the law to be an impermissible content-based restriction on speech, overly broad and unconstitutionally vague.

3. In ***Urofsky v. Gilmore,*** 167 F.3d 191 (4th Cir. 1999), an appellate panel reversed a ruling by District Court Judge Leonie Brinkema that had struck down a Virginia statute that restricted the ability of state employees to access sexually explicit material on state owned or leased computers.

4. In ***ACLU v. Johnson,*** 4 F. Supp. 2d 1029 (D.N.M. 1998), the court enjoined enforcement of a New Mexico statute intended to protect children from sexually explicit Internet content, finding the law unconstitutional under the First, Fifth and Fourteenth Amendments and the Commerce Clause of the U.S. Constitution.

G. International Regulation of Offensive Material.

1. **Germany.** In response to a claim from federal prosecutors in Germany that the pornographic content of certain Internet newsgroups violated German law, CompuServe temporarily blocked access to as many as 250 Internet newsgroups from its worldwide network in late 1995, because it could not block access solely to its German subscribers. In early 1996, the prosecutor's office in Mannheim, Germany launched an investigation of CompuServe and Deutsche Telekom's T-Online service for inciting racial hatred because these online services, as Internet providers, allow Germans to access a website run by a neo-Nazi extremist in Canada who uses the Internet to distribute anti-Semitic propaganda. Edupage, Jan. 28, 1996, *citing The Wall Street Journal,* Jan. 26, 1996, at B2. The former head of CompuServe's German division ultimately was found guilty of willful distribution of pornographic material, given a two year suspended sentence, three years probation

and fined 100,000 Deutsche Marks. Some have argued that the conviction will likely be overturned on appeal. *See, e.g.,* Daniel Nathrath, "Criminal Liability of Internet Providers in Germany: Conviction of a CompuServe Executive," J. Internet L., Nov. 1998, at 1.

2. **Singapore.** In March 1996, the government of Singapore notified Internet content and access providers in that country that it would hold them responsible for voluntarily restricting pornographic and politically objectionable material in transmissions to the country's estimated 100,000 accounts. Edupage, Mar. 7, 1996, *citing W.S.J.,* Mar. 6, 1996, at B6.

3. **The P.R.C.** The P.R.C. has banned online pornography and all political discourse, and requires all computer networks in that country to register with the government. All international Internet access must be coordinated through China's Ministry of Posts and Telecommunications. Edupage, Feb. 6, 1996, *citing The New York Times,* Feb. 5, 1996, at A1. There are an estimated 50,000 Internet accounts in the P.R.C. *Id.*

Next Section / Contents

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

XIII. INTERNET CRIMES

A. Criminal Copyright Infringement

See the Net Act, *supra* § II(I).

B. Fraud and Abuse Act of 1986

1. 18 U.S.C. § 1030(a)(5)(A) penalizes "anyone who intentionally accesses a Federal interest computer without authorization, and by means of one of more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information . . ." and thereby causes loss of $1,000 or more.

2. In ***United States v. Morris,*** 928 F.2d 504 (2d Cir.), *cert. denied,* 502 U.S. 817 (1991), the Second Circuit upheld the conviction under this act of Robert Morris, a Cornell graduate student who released the Internet "worm," which was a virus that replicated itself multiple times over the Internet causing computers around the country to crash, including government computers.

C. Threats Transmitted Via Email

1. ***United States v. Baker,*** 890 F. Supp. 1375 (E.D. Mich. 1995), *aff'd sub nom. United States v. Alkhabaz,* 104 F.3d 1492 (6th Cir. 1997).

a. **Indictment quashed.** The court granted the defendant's motion to quash his indictment under 18 U.S.C. § 875(c) for five counts of transmitting threats to injure or kidnap another in email messages transmitted over the Internet to "Gonda," an anonymous cyberfriend in Canada. Baker had posted a "rape fantasy" story to an Internet newsgroup, which graphically described the torture, rape and murder of a woman who was given the name of a classmate of Baker's at the University of Michigan. During the course of the investigation into this incident, Baker consented to a search of email messages stored on the hard drive of his dormitory room computer.

b. **Threats too remote.** The court determined that the messages sent by private email did not amount to threats when evaluated in light of their foreseeable recipient (an anonymous email correspondent). As an illustration of the potential difficulties associated with applying existing laws to cyberspace, the court wrote that "'he' could be a ten year old girl, an eighty year old man, or a committee in a retirement community playing the role of Gonda gathered around a computer."

2. **Stalking laws.** Sending harassing email messages could violate California's stalking law or analogous statutes enacted in other states. See Cal. Penal Code § 646.9 (declaring it illegal to willfully, maliciously and repeatedly follow or harass another person and make a credible threat with intent to place that person in reasonable fear of death or bodily injury); McGraw, "Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail," 20 Rutgers Computer & Tech. L.J. 491 (1995).

D. Trade Secrets

The Economic Espionage Act of 1996 criminalizes wrongful copying or control of trade secrets. 18 U.S.C. § 670.

1. A trade secret is defined under the Act to mean all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public . . .

2. The statute criminalizes two types of misappropriations where the defendant has "wrongfully copie[d] or otherwise control[led] a trade secret, or attempt[ed] or conspire[d] to do so . . ." First, the law proscribes wrongful copying or control where the defendant has reason to believe that the offense will, or where the defendant actually intends to, "benefit any foreign government, foreign instrumentality, or foreign agent . . . " Second, the statute prohibits wrongful copying or control "with the intent to divert a trade secret, that is related to or is included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and with the intent to, or reason to believe that the offense will, disadvantage any owner of the trade secret . . ." 18 U.S.C. § 670(a).

E. The National Stolen Property Act

1. **Electronic theft covered by the act: *United States v. Riggs,*** 739 F. Supp. 414 (N.D. Ill. 1990).

> a. **Facts:** Neidorf and Riggs accessed Bell South's computer and transferred certain files via modem to Neidorf's computer. Defendants were convicted under 18 U.S.C. § 2314 for theft of electronic text files.
>
> b. **Conviction.** The court reasoned that because "[i]t is well-settled that when proprietary business information is affixed to some tangible medium, such as a piece of paper, it constitutes 'goods, wares or merchandise' within the meaning of Section 2314, and because Riggs' conduct clearly would have come within the statute if the files he had stolen had been affixed to a floppy disk or printed in hard copy, "[t]his court sees no reason to hold differently simply because Neidorf stored the information inside the computer instead of printing it out on paper. In either case, the information is in a transferable, accessible, even salable form." *Id.* at 420-21. In the alternative, the court ruled that the

information was tangible property:

> Although not printed out on paper, a more conventional form of tangibility, the information in Bell South's E911 text file was allegedly stored on a computer. Thus, by simply pressing a few buttons, Neidorf could recall that information from computer storage and view it on his computer terminal.

c. **First Amendment defense rejected.** Riggs' First Amendment defense subsequently was rejected in *Riggs v. United States,* 743 F. Supp. 556 (N.D. Ill. 1990).

2. **Electronic theft not covered by the Act: *United States v. Brown,*** 925 F.2d 1301 (10th Cir. 1991).

a. **Holding:** The Tenth Circuit held that a computer program (including source code and documentation) were intangible property and, as such, did not constitute "goods, wares, merchandise, securities or monies" which had been stolen within the meaning of the National Stolen Property Act, 18 U.S.C. §§ 2311 *et seq.* 925 F.2d at 1307-09.

b. ***Riggs* analysis rejected.** The Tenth Circuit expressly declined to follow *United States v. Riggs* because it found that the statute covered only *physical*, not intangible "goods, wares [or] merchandise." *Id.*

F. Wire Fraud

A district court held that a defendant was properly charged under the wire fraud statute for the alleged transmission of computer files containing source code, over the defendant's objection that he should have been charged only with copyright infringement. The court noted that the wire fraud statute, 18 U.S.C. § 1343, contains no requirement that physical goods or money be involved. *United States v. Wang,* 898 F. Supp. 758 (D. Colo. 1995).

G. Civil Remedies for Unlawful Seizures

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

1. **Facts:** Steve Jackson Games, Inc. ("SJG") published books, magazines and games and operated a BBS called "Illuminati," which it used to post public information about its business, facilitate testing of games in development and communicate with its customers by email. After obtaining a search warrant based in large part on information about an unrelated BBS, the U.S. Secret Service seized SJG computers, disks and electronic "manuscripts" about to be published and, instead of copying the data and returning it, held onto the material for more than three months. The Secret Service also read and deleted private email messages addressed to BBS subscribers, which had been stored on one of the seized hard disk drives.

2. **The Federal Wiretap Act** (18 U.S.C. § 2510), as amended by title I of the Electronic Communications Privacy Act of 1986 ("ECPA"), proscribes intentional interceptions of wire, oral or electronic communications. The Fifth Circuit held that the seizure of a computer on which private email has been stored (but not yet retrieved by the intended recipients) does not constitute an unlawful "intercept" under the Federal Wiretap Act.

3. **The Privacy Protection Act** (42 U.S.C. §§ 2000 *et seq.*) makes it unlawful for a government employee to seize, in connection with a criminal investigation, any

materials "reasonably believed to have a purpose to disseminate to the public a newspaper, broadcast or similar form of public communication . . . ." 42 U.S.C. § 2000aa(a). The trial court previously had found that the Secret Service's failure to promptly make copies of draft magazine articles and a book intended for publication, after being advised that the materials were to be published, constituted a violation of the Act (despite the individual officers' protest that they had no actual knowledge of the Act), justifying an award of $51,040 in damages. 816 F. Supp. 432, 440 (W.D. Tex. 1993), *aff'd,* 36 F.3d 457 (5th Cir. 1994). The government abandoned its cross-appeal of this issue.

4. **Stored Wire and Electronic Communication**s (18 U.S.C. §§ 2701 *et seq*.). Title II of the EPCA proscribes unauthorized intentional access to stored electronic communications. The district court previously held that the Secret Service had violated this Act and awarded plaintiffs statutory damages and attorneys' fees. The government abandoned its cross-appeal of this issue.

H. Use of the Internet for Law Enforcement

The first criminal charges brought based on an Internet wire tap were filed in early 1996 by the U.S. attorney in Brooklyn, New York against two Americans and a German national who were charged with illegally making and selling electronic devices and cloning equipment used for cellular telephones. Intellectual Property Lawcast, Jan. 15, 1996. The wiretap was obtained following a complaint by AT&T that cellular telephones programmed with stolen numbers were advertised for sale on a worldwide website. Cyberlex (Jan. 1995), *citing The New York Times,* Dec. 30, 1995, at A22.

Next Section / **Contents**

E-Commerce and Internet Law: A Primer

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

(continued)

XIV. JURISDICTION

A. Personal Jurisdiction

1. **Constitutional Test.** A court may exercise "general jurisdiction" over a defendant if the nonresident defendant's activities within the forum are "substantial" or "continuous and systematic." *Helicopteros Nacionales de Colombia, S.A. v. Hall,* 466 U.S. 408, 414 n.9 (1984), *citing Perkins v. Benguet Consolidated Mining Co.,* 342 U.S. 437, 445 (1952). Alternatively, a court may obtain "specific jurisdiction" over a nonresident defendant if the defendant has sufficient contacts with the forum state and the cause of action to satisfy the "minimum contacts test" first articulated by the *U.S. Supreme Court in International Shoe Co. v. Washington,* 326 U.S. 310 (1945). In that case, the Court held that:

> [D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present with in the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice."

Id. at 316, *citing Milliken v. Meyer,* 311 U.S. 457, 463 (1940); *see also World Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980).

2. **Contracts**

a. In ***CompuServe, Inc. v. Patterson,*** 89 F.3d 1257 (6th Cir. 1996), the Sixth Circuit held that an Ohio court could assert personal jurisdiction over a Texas resident who had entered into an electronic commercial contract with CompuServe from his home in Texas, to market his shareware software programs.

b. In ***Hall v. LaRonde,*** Cal. App. 4th 1342 (1997), a state court in California held that email communications may form the basis for the assertion of jurisdiction.

3. **Operation of a website**

a. Early decisions held that a defendant's mere operation of a website to promote its business which could be accessed by residents of the forum state, was sufficient to confer specific jurisdiction in a dispute arising out of the domain name used in connection with the site. *See, e.g., Inset Systems, Inc. v. Instruction Set, Inc.,* 937 F. Supp. 161 (D. Conn. 1996); *Panavision Int'l, L.P. v. Toeppen,* 938 F. Supp. 616 (C.D. Cal. 1996); *Maritz, Inc. v. CyberGold, Inc.,* 947 F. Supp. 1328 (E.D.

Mo. 1996). *But see The Hearst Corp. v. Goldberger,* Case No. 96 Civ. 3620 (S.D.N.Y. Feb. 26, 1997) (analogizing a website to an advertisement in a national publication and following *Bensusan*).

b. Other courts found jurisdiction proper where a defendant also had more traditional contacts with the jurisdiction. *See, e.g., Heroes, Inc. v. Heroes Foundation*, 958 F. Supp. 1 (D.D.C. 1996) (newspaper advertisement); *Zippo Mfg Co. v. Zippo Dot Com, Inc.,* 952 F. Supp. 1119 (W.D. Pa. 1997) (contracts with forum residents and forum subscribers); *Digital Equip. Corp. v. AltaVista Technology, Inc.,* 960 F. Supp. 456 (D. Mass. 1997) (license agreement).

c. In ***Bensusan Restaurant Corp. v. King,*** 126 F.3d 25 (2d. Cir. 1997), the court held that the defendant's mere establishment of a website that was accessible to New York residents, without more, was insufficient to confer specific jurisdiction over a nonresident defendant under New York's long arm statute, in a lawsuit arising out of rights to a trademark used on the defendant's website. The court did not reach the constitutional question of whether jurisdiction would have been proper under the minimum contacts test.

d. In ***Cybersell, Inc. v. Cybersell, Inc.,*** 130 F.3d 414 (9th Cir. 1997), the Ninth circuit held that a defendant's mere presence on the World Wide Web is insufficient to confer jurisdiction under the minimum contacts test. Applying the analysis first adopted in *Zippo Manufacturing Co. v. Zippo Dot Com.,* 952 F. Supp. 1119 (W.D. Pa. 1997), the Ninth Circuit distinguished between passive websites, which are merely akin to advertisements, and interactive sites. Under the *Cybersell/Zippo Dot Com* test, jurisdiction may obtain over a defendant based solely on its operation of a website depending on "the level of interactivity and [the] commercial nature of the exchange of information that occurs on the website." 952 F. Supp. at 1124. The *Cybersell/Zippo Dot Com* test is now the leading standard applied by U.S. courts.

e. In ***Panavision Int'l, L.P. v. Toeppen,*** 141 F.3d 1316 (9th Cir. 1998), the Ninth Circuit held an out-of-state cybersquatter subject to jurisdiction in California under the effects test of *Calder v. Jones*, 465 U.S. 783 (1984).

B. U.S. Customs Law

Customs exclusion orders barring the importation of products bearing marks identical to registered U.S. trademarks, or protected by U.S. copyrights (15 C.F.R. §§ 133.15 to 133.21 and 133.31 to 133.37) are rendered meaningless for certain goods (notably software, books and magazines) which can be transmitted over the Internet.

C. Criminal Law

In July 1994, Carleen and Robert Thomas, a Milpitas, California couple who operated a BBS that allowed subscribers to download sexually explicit material, were convicted of interstate transportation of obscene material based on their operation of the BBS. The venue for the trial was in the Western District of Tennessee, where a postal inspector initiated a telephone call to the BBS and where community standards were considered to be more likely to favor a conviction. U*nited States v. Thomas,* 74 F.3d 701 (6th Cir. 1996).

D. Attorney Advertising

The ethical standards for lawyer advertising are established separately by regulatory authorities in each state. Two states, Texas and Florida, require that home pages be submitted for approval, while other states do not. The jurisdictional reach of these two state requirements is not entirely clear.

1. **Texas** After being chastised in a reported decision for adopting new ethical guidelines that failed to consider advertising over the Internet (*Texans Against Censorship, Inc. v. State Bar of Texas,* 888 F. Supp. 1328, 1370 (E.D. Tex. 1995), *aff'd mem.,* 100 F.3d 953 (5th Cir. 1996)), the State Bar of Texas adopted a rule requiring Texas lawyers to file a hard copy of their home pages (and printouts showing any subsequent material changes). *See* State Bar of Texas, Interpretive Comment 17.

2. **Florida.** Attorneys must submit a hard copy of their homepages, the URL and a check for $100. The Standing Committee on Advertising, "Internet Guideline," **http://ww3.pwr.com/LEGAL/FLABAR/Regulations/AdReg/adguide.html**.

3. **North Carolina.** In a proposed ethics opinion, the North Carolina Bar Association concluded that the requirement that attorneys retain records of their advertisements may be satisfied by printing out every single page on a website as launched and all subsequent material changes and retaining the printouts for two years. Proposed RPC 239 (July 25, 1996).

E. Tax Law in Cyberspace

1. **The Internet Tax Freedom Act.**

a. **Moratorium.** In late 1998, Congress imposed a three year moratorium on the imposition of new state or local taxes, including (1) certain Internet access taxes, (2) bit taxes; or (3) multiple or discriminatory taxes on electronic commerce. The Internet Tax Freedom Act also established the Advisory Commission on Electronic Commerce to study and report to Congress on federal, state and international taxation and tariff treatment of Internet transactions or access.

b. **Exclusions.** The moratorium does not have any effect on state or local taxes "generally imposed and actually enforced prior to October 1, 1998 . . . ." The Act likewise is not intended to have any retroactive effect on liability for taxes "accrued and enforced before the date of enactment" of the Act or have any effect on ongoing litigation relating to such taxes.

c. **Exemption.** An exemption to the moratorium exists in the case of any person or entity who in interstate or foreign commerce is "knowingly engaged in the business of selling or transferring, by means of the World Wide Web, material that is harmful to minors . . . ," except where the use of a verified credit card, debit account, adult access code or adult personal identification number (or alternative procedures to be prescribed by the FCC) to restrict access to people under 17 years old. Excluded from this category of persons (and therefore eligible to benefit from the moratorium) are:

- Telecommunications carriers engaged in the provision of a telecommunications service;
- Persons engaged in the business of providing Internet access services;

- Persons engaged in the business of providing Internet information location tools; or
- Persons "similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation . . . of a communication made by another person, without selection or alteration of the communication."

2. **Tax compliance.** As electronic commerce increases, tax compliance may become more difficult to monitor. Some have argued that the Clinton Administration's reluctance to ease export restrictions for encryption technology is based in part on concern for the IRS' ability to monitor compliance. As explained by one economist, "electronic money gets really interesting when you realize how impossible it is to put national walls around it, mandate the use of national currencies, or require that transactions go through banks. . . . A country will have no practical choice but to rely more than ever on voluntary tax compliance." Edupage Jan. 9, 1996, *citing Investor's Business Daily,* Jan. 9, 1996, at B1

F. International Government Regulation of the Internet

In addition to the U.S. government's NII White Paper, other governments have issued reports on the Internet.

1. **Canada.** The Final Report of the Information Highway Advisory Council may be found at **http://www.emp.ca/opengov/nabst**.

The Canadian government's response can be found at **http://info.ic.gc.ca/info-highway/society/toc_e.html**.

2. **EEC.** The EEC Action Plan can be found at **http://www.echo.lu/eudocs/en**.

3. **Australia (with links to other international reports).** The Australian government has set up a home page on the World Wide Web with links to many other government reports. That web page is located at **http://www.nla.gov.au/lis**.

Next Section / **Contents**

E-Commerce and Internet Law: A Primer

Ian C. Ballon
Manatt, Phelps & Phillips, LLP
iballon@manatt.com

The 2nd Annual Spring Meeting

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

(continued)

XV. UPDATE INFORMATION AND NEW CASE LAW

This outline is updated periodically to account for the rapid transformations taking place in the emerging field of Internet law. To request a free update, email your name, address and phone number to IanBallon@Manatt.com.

Contents

The 2nd Annual Spring Meeting BUSINESS LAW SECTION